The Art of Balancing Information Security and Information Sharing

Michael Cartney

March 2000

Program On Information Resources Policy

Harvard University
Cambridge, Massachusetts

Chairman
Anthony G. Oettinger

Managing Director
John C. B. LeGates

A research draft of the Program on Information Resources Policy. Research drafts are works in progress. They are not for sale, nor are they to be cited or copied without prior written permission.

Copyright @2000 by the President and Fellows of Harvard College. Not to be reproduced in any form without written consent from the Program on Information Resources Policy, Harvard University, 33 Oxford Street rm 125, Cambridge, Ma, 02138. (617) 495-4114. www.pirp.harvard.edu

20010921 135

DISTRIBUTION A:

Approved for public release; distribution is unlimited.

Air Force Fellows Program
Maxwell AFB, Al 36112

Acknowledgements

The author gratefully acknowledges the following people who were interviewed, reviewed and commented critically on the draft version of this document. Without their consideration, input, and encouragement, this study could not have been completed.

General(ret) T Robert Marsh

Dr James Hearn

Col David Komar

Ms Virginia Wiggins

Gen (ret) James Clapper

Lt Gen John Woodward

Dr Charles Popper

Col H Gordon Thigpen

Dr Robert Beck

Lt Gen Albert Edmonds

The reviewers and the Program Affiliates, however, are not responsible for, or necessarily in agreement with, the views expressed here, nor should they be blamed for any errors of fact or interpretation.

Executive Summary

Balancing the needs of information sharing against threats to security is an age-old dilemma; operational security (OPSEC) often conflicts with operational effectiveness; protecting intelligence sources and methods may undermine confidence in the product; and guarding trade secrets and customer privacy may prevent the introduction of e-commerce innovations. But in today's global, high-tech, information-oriented environment, with exploding demands for both information sharing and information security, the importance of getting a better balance between information sharing and security is becoming critical to survival.

When is an information environment so open that openness jeopardizes vital interests? How much *ought* security impede effectiveness? How are these crucial but often conflicting requirements to be weighed? Who are the stakeholders, and what are the stakes? What are the trade-offs? Where does technology fit in? Where is each organization's balance between information sharing and information security? These are all crucial questions that are often left unanswered or incomplete in many of organizational approaches to IS&S. However, the focus of the framework presented here is not on specifically answering these questions, but rather, on how organizations can better ask and address them.

The original framework developed in this project and described here suggests ways for organizations to improve their approaches to information sharing and security (IS&S) by looking beyond the traditional security paradigm and using a framework that remains rooted in, and focused on, the operational aspects of how (business culture) and why (business value) organizations do business. It does so by:

- linking the objectives of IS&S to overall business objectives and how these objectives are managed on the basis of business value;
- recognizing the essential role of business culture by emphasizing enterprise-wide participation, understanding, and support of IS&S;
- developing an IS&S approach by examining and weighing influences and options based upon business value; and
- evaluating and managing IS&S efforts from an enterprise-wide perspective.

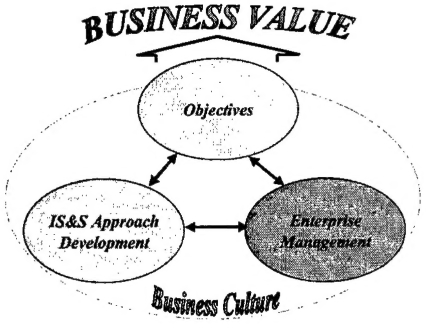


Figure 1 -The Information Sharing and Security Model

Adhering to these guidelines, the framework described enables organizations to better practice the art of balancing information sharing against information security by providing them with the tools and concepts needed to identify, capture, focus, and address influences on IS&S.

By using business value as the common denominator for measuring expectations, analyzing options, and assessing influences, the framework helps both in balancing security against sharing and enables security and sharing efforts to be balanced within the overall business model. Recognizing the context of business culture and its impact on every aspect of the approach to IS&S allows each business to develop a more usable approach. It presents strategies and tools for use in identifying and then developing measurable IS&S objectives and in examining several key influences on decisions about IS&S. The framework offers insights into how to identify and analyze the influences affecting an approach to IS&S: influences that include business culture, objectives, stakes and stakeholders, technology, trends, and vulnerabilities. Finally, the model outlines an approach to the management of IS&S that is both inclusive—whose scope truly reflects the potential contribution of information—and more specific, by going beyond attractive theories to specific, business-related measures and directly incorporated IS&S into the overall enterprise management process.

Whether they are a small startup information-technology company considering what to tell potential strategic partners or the U.S. government deciding what military intelligence information to share with allies and potential coalition partners, every organization faces the enormous challenges of finding their sharing and security balance. By understanding the term *business* in a generic sense, as meaning *getting something accomplished*, and *operations* and *operational aspects* as meaning *the activities required to accomplish something,* the proposed framework developed here becomes applicable to all types of businesses. By plugging in its own specific terminology, any group can tailor the framework to make it relevant to its particular business—whether it be diplomacy, manufacturing, finance (including sales and e-commerce), education, consulting, or any other type of activity.

Table of contents

FIGURES (page number)

TABLES (page number)

The Art of Balancing Information Security and Information Sharing

Michael Cartney

December 1999

Information sharing is like breathing — you have to do it to survive. How well you do it affects your strength, but, if you overdo it you will pass out. And you have to be careful what you breathe.

■ General (ret) R Thomas Marsh, Chairman, PCCIP[1]

■

"As we wire the world and our lives, we add new vulnerabilities that will be exploited. As a country and a society, we have no desire to stop, or even slow down, the dramatic technological improvements that the information revolution offers. Nonetheless, as we incorporate new systems into our lives and as we become increasingly dependent upon them, we must be prepared to protect ourselves."

■ Project Air Force, 1999[2]

I. Chapter 1 – The Framework at a Glance

Balancing the needs of information sharing against threats to security is an age-old dilemma; operational security (OPSEC) often conflicts with operational effectiveness; protecting intelligence sources and methods may undermine confidence in the product; and guarding trade secrets and customer privacy may prevent the introduction of e-commerce innovations. When is an information environment so open that it jeopardizes vital interests, and how much should security impede effectiveness? Amplifying the complexity and importance of the question is the fact that today's global, high-tech, information-oriented environment is characterized by exploding demands for both information sharing and security (IS&S). How are these crucial but often conflicting requirements to be weighed? Who are the stakeholders involved, and what are the stakes? What are the tradeoffs? Where does technology fit in? Where is the organization's balance between information sharing and information security?

The focus of this study is not on directly addressing these difficult questions, but rather on developing the framework in which organizations can ask and address them. The original

[1] Gen Marsh, in interview with the author, 16 December 1999.

[2] Zalmay Khalilzad in Chapter Fourteen of RAND's 1999 Project Air Force Book, "Strategic Appraisal: The Changing Role of Information in Warfare", <u>*Defense in a Wired World: Protection, deterrence, and prevention*</u>

framework which follows provides ideas and tools for examining the questions: 1) why do we share information? 2) Why do we secure information? 3) What should play a role in our decisions when there is business value in easily sharing information and there is also business value in restricting the free flow of the information? And 4) How much is too much sharing and how much is too much security? These are enormous questions faced by every organization, whether it is a small start up information technology company considering what it should tell potential strategic partners, or the US government deciding what military intelligence information to share with Allies and potential coalition partners. By taking *business* in the generic sense as meaning *getting something accomplished,* and *operations* and *operational aspects* as meaning the *activities required to get something accomplished,* the framework proposed and developed in this paper becomes applicable to all types of business. By plugging in a particular group's terminology they can make the framework relevant to their *business.* Diplomatic, financial, sales, manufacturing, e-commerce, education, consulting, literally any type of *business*, will find the framework useful.

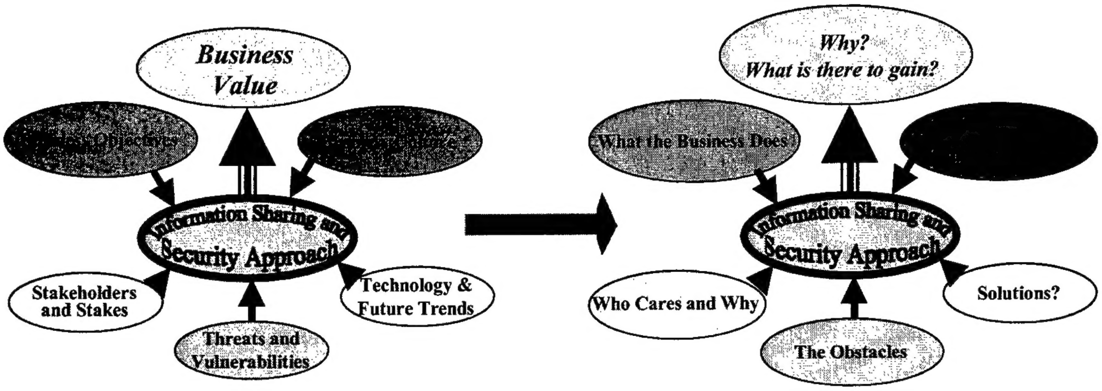

Business Value
Objectives
Information Sharing and Security Approach
Stakeholders and Stakes
Threats and Vulnerabilities
Technology & Future Trends
Why? What is there to gain?
What the Business Does
Information Sharing and Security Approach
Who Cares and Why
The Obstacles
Solutions?

Figure 1 - Information Sharing &Security (IS&S) Approach Influences

The framework provides thoughts on identifying and analyzing the influences (see Figure 1) on the information sharing and security (IS&S) approach: Business culture, Objectives, stakes and stakeholders, technology, trends, and vulnerabilities. The paper presents thoughts and tools for developing information sharing and security objectives, examining the roles of several key influences on information sharing and security decisions. Then, the role of stakeholders and their stakes in the approach to information sharing and security is examined. Next, identifying threats and vulnerabilities to security and sharing are addressed. The issues of the fluid technology based business and information worlds are examined, providing ideas for addressing the dynamic nature of threats, vulnerabilities, information uses, information value, information quality and the business environment from an information sharing and security perspective. Finally, ideas on incorporating IS&S into the overall enterprise management processes are presented.

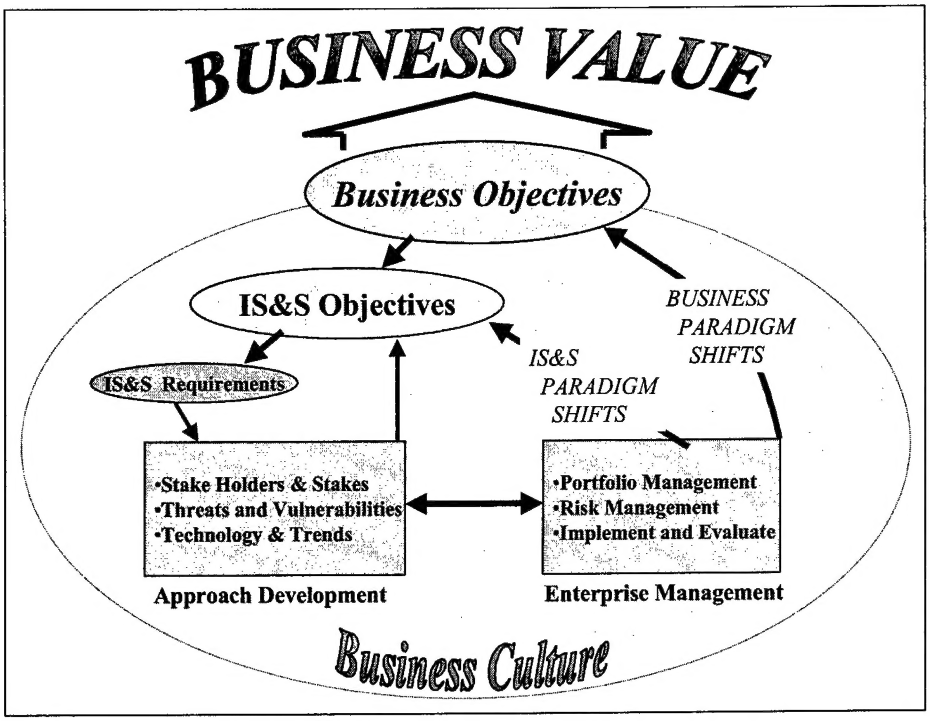


Figure 2- Information Sharing and Security (IS&S) Approach Development Process

The original framework, developed and described in this paper, enables organizations to practice the art of balancing information sharing and security by providing tools and thoughts for identifying, capturing, focusing, and addressing the information sharing and security influences presented earlier. As depicted in Figure 2, the paper investigates the benefits of an information sharing and security framework that is rooted in, and remains focused on, the operational aspects of how (business culture) and why (business value) business is done by:

1. linking the objectives of IS&S to overall business objectives and how these objectives are managed on the basis of business value;
2. recognizing the essential role of business culture by emphasizing enterprise-wide participation, understanding, and support of IS&S;
3. developing an IS&S approach by examining and weighing influences and options based upon business value; and
4. evaluating and managing IS&S efforts from an enterprise-wide perspective.

Using business value as the common denominator for analyzing and assessing the various influences, the framework not only helps in balancing security against sharing, but also enables security and sharing efforts to be more easily balanced within the larger business model. Recognizing the context of business culture and how it impacts every aspect of the IS&S approach enables the development of a more usable approach.

Even the wording of the question or task can imply whether the emphasis of the organization is primarily to share or secure its information. Is the organization's approach to sharing and security permissive or restrictive in nature? The difference can be as minor looking as asking what information can be shared versus what information must be shared. In a permissive information sharing environment, information is shared unless there is a reason not to. In the restrictive environment, information is shared only when there is a reason to. In a permissive security environment, the default is to not secure information. In a restrictive security environment, the default is to secure the information. Which formulation is correct will be a dynamic of the business's culture.

To illustrate and clarify the framework, two sample scenarios are used to illustrate, highlight, and clarify certain of its aspects. Owing to the author's background, the perspective is of military automated data processing (ADP) information systems, but both the framework and the concepts are applicable to government and business information systems in general.

A word about the samples: More detailed synopses of the sample scenarios are available in Appendix B of this paper.

Sample Scenario 1: As outlined in both Presidential Directive (PDD) 62 and PDD 63, the challenges of information warfare, cyber terrorism, and cyber crime are blurring the boundaries between law enforcement, intelligence, State, Defense, state governments, local governments, and the private sector concerning their roles and responsibilities for protecting the national information infrastructure. PDD 63 requires a supporting 'detection, warning and response' information network to protect the National Information Infrastructure (NII) by enabling: detection, warning, and thwarting of attack; investigation and determination of response; and rapid response and recovery. To a large extent, PDD 62 requires the same entities to be interconnected to support information sharing about, and responses to, terrorism. This paper uses the question "Is there a feasible approach to connect the major players and share key information electronically," to highlight and discuss the associated sharing and security issues.

Sample Scenario 2: As information requirements and the volume of data grow, as concerns in information sharing and security broaden, as response times become shorter and shorter, and as "cyber threats" and "information targets" expand, will the Department of Defense (DOD) need to balance information security and information sharing for its concepts for the 21st century to be feasible? Some areas come in for extensive discussion: Information Warfare, interoperability, Battle Space Dominance, Rapid Response, integration of air and space assets, combined Information Operations. But the element missing from these discussions is a clear and comprehensive, workable approach to information sharing and security. Will the DOD's Joint Command and Control Infrastructure security approach meet the needs of tomorrow? For the purposes of this paper, discussion will be limited to objectives, stakeholders, stakes, trends, and assessments pertaining to the Global Command and Control System/Global Combat Support System (GCCS/GCSS) security approach of maintaining separate security classification levels on disjoint, separate networks versus connecting or bridging the networks and employing a data confidentiality labeling scheme.

This paper does not propose a security approach and direction for either the Global Command and Control System or the National Information Infrastructure. It develops the framework in which those decisions can be made and implemented. In both samples, the information systems have three ingredients that are common to all information systems facing the sharing/security issue: 1) information at differing levels of confidentiality; 2) increasing reliance on the quality and quantity of information to be shared; and 3) existing and potential threats to that information. These common ingredients are important because they make the underlying issues examined generally applicable to any public or private organization.

Chapter 2 – Why Share? Why Secure?

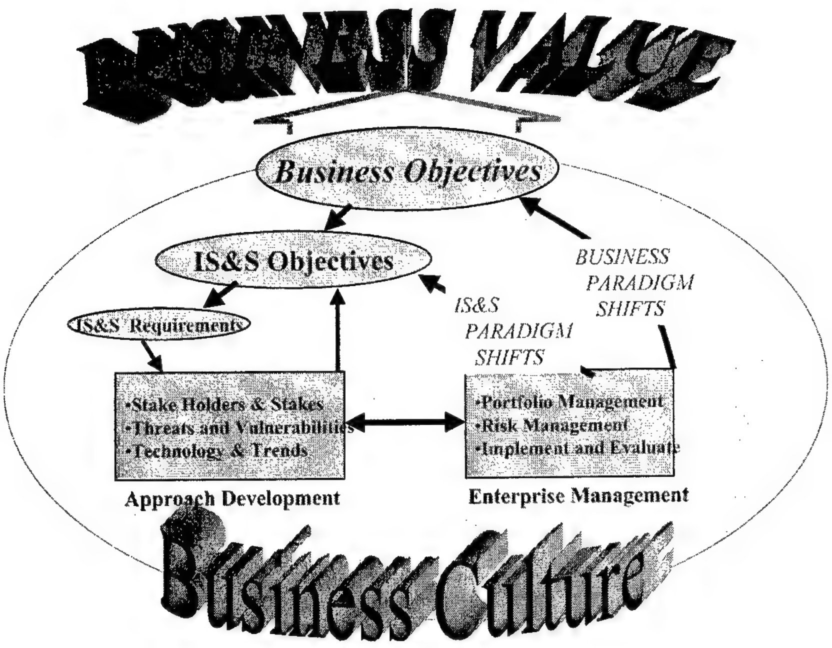


Figure 3 - IS&S: Achieving Business Value within the Business's Culture

Is Information Age business about free and open exchange of information or it is about rapid, seamless, and controlled information usage between business entities? If we are addressing security, then there are entities that we need to prevent from accessing, manipulating, or interfering with information flows. But why? Why do we share information? Why do we secure information? What is our motivation for either of these activities? In examining these questions, the specific answers always point to one general answer, 'because it is good for the business.' Information is shared because it brings direct or indirect benefits to the business. Sometimes the benefit of sharing stems from the value of the information, but sometimes the benefit results from the act of sharing itself. Information is secured because there is some legal, political, or operational benefit to doing so. Would organizations expend precious resources on these activities if they did not benefit the business? But even the business value of information is dependent on the business culture. As depicted in figure 3, whatever process is outlined for information sharing and security (IS&S), the goal is business value, and the process operates against the backdrop of business culture. Consequently, one of the first activities in developing an information sharing and security approach is defining what there is to gain, what is the business value, or more succinctly, why.

1. Business Value – A Common Thread

This paper is based upon the premise that the underlying motivation for business activities is gaining or retaining business value. Not only is this common motivation important in capturing, clarifying, and focusing analysis of influences, but it also provides a viable means by which to accurately compare the impacts of influences. Unfortunately, there is no standard definition of business value. Dependent on the type of enterprise, business value can be as straightforward as cash flow and efficiency/effectiveness of operations, or as complicated as strategic international relationships. The specific meaning of business value depend on the enterprise, its business objectives, and the specific question or circumstances. However, since business value is the common thread across the influences, a consistent, common understanding is important.

Using information value as the common thread is also possible. However, two things need to be considered in this choice. First, like business value, there is no standard definition for information value and information value would ultimately need to be expressed in business value terms to be meaningful to the organization. Additionally, since business value is broader than information value, cases may be found where different options or aspects result in the same information value, but differing business values. Therefore, while defining and assessing information value may be helpful to aspects of various assessments, such as which information products are worth protection, using information value as the common thread could diminish the quality of the overall analysis.

In addition to enabling comparisons, using business value as the common thread has other advantages. As seen below, a common thread helps to focus the collection and analysis of the influences to those items having the biggest impact on accomplishing the business objectives. But, perhaps more important, by discussing influences in business terms, information sharing and security's impact on and importance to the organization may be more easily and more fully understood by upper management. Finally, another benefit is that by performing business value based analysis, information sharing and security advocates could more easily develop business impact cases in term of business advantages, returns on investment, and cost/benefits analysis as well as less tangible aspects such as customer confidence, business reputation, and long term business impacts.

A brief example. In business value terms, anti-virus software can be described as an inexpensive, effective solution that ensures business days are not unnecessarily lost to an avoidable, but highly likely, near-term threat that could interrupt all operations supported by computer systems (95% of the corporation) which has a 100 to 1 estimated return on investment ratio. In more technical terms, anti-virus software can be described as an inexpensive, effective tool that detects and remedies malicious software capable of corrupting databases, interrupting e-mail, and even crashing computer systems. Which description is more likely to be understood, supported, and funded by upper management?

A more difficult example is the characterization of business value for the sample scenario 1, the PDD scenario. Getting agreement on the definition of business value in such a diverse environment could be a major achievement. Later, in the discussion on stakeholders and culture, we will see that the various parties have extremely different views on what is important and on what they are trying to achieve. Even a generic specification of business value such as "gaining or maintaining business opportunities while increasing information sharing and maintaining or increasing information security" may not be agreed to. That is because phrases such as "business opportunities" may mean one thing to some government entities, something else to other government agencies, and something different yet to industry. If the government wants industry to actively participate, will they have to formulate the goals of the effort, not particularly in terms of benefit to the government, but in terms that accent the value to industry and to the American People? Are there benefits to this type of approach and would such an approach force the government to think, plan, and discuss the topic differently? Would the PDD effort be less open to criticism such as that of Peter Daly when he states, "The PDD suggests the creation of an elaborate, government led, public-private partnership structure that depends heavily on intra-sector information exchange and centralized government decision-making on risk and response.

But, while the Commission's report and resulting PDD talk a lot about new paradigms and new ways of managing risk, it recommendations relate almost exclusively to vestigial concepts of defending the shores and apprehending criminals.[3]"?

For the GCCS scenario, the Chairman of the Joint Chiefs of Staff (CJCS) defines business value as moving the military toward "...a joint force — persuasive in peace, decisive in war, and preeminent in any form of combat."[4] More specific to GCCS, the Joint Staff's Director for Command, Control, Communications, and Computer Systems, and his four Service counterparts, define business value in *C4I for the Warrior* as something that "...brings to the warrior an accurate and complete picture of the battle space, timely and detailed mission objectives, and the clearest view of their targets."[5] For the purposes of the sample scenario, these measures will be used.

2. The relationship of business culture to information sharing and security approaches.

Information security will only pay off if it is designed and managed with the recognition that it must be based upon the culture and politics of the enterprises it is intended to support[6]

Information sharing and security affects virtually every aspect of the business. Accordingly, the business culture, how the organization works, can impact ever aspect of information sharing and security. In examining the business culture, it is just as important to understand why the organization works the way it does as it is to understand how the organization works. Without accounting for the business culture, an approach that is in every other way sound, may be unusable or untenable within a certain organization.

For instance, the military installed secure telephone technology to increase security during operations. During peacetime, the usage rate of the secure phone was relatively high. However, at the start of the next major military operation, when one would expect security to increase, use of the secure features of the phone dropped significantly[7]. Whether the drop in use was intentional because of perceived time constraints or unintentional, the security approach did not fit into the military's operational culture, and was therefore by-passed.

Business culture is interwoven throughout the organization and its tasks. Even something as basic as the wording of the information sharing and security task or question is an opportunity to reflect the organization's objectives, philosophy, and direction. Will the effort be focused on determining what information to share or on determining how to best secure the environment? Will the propensity be towards sharing or with holding information? Is the idea to emphasize or de-emphasize security? All these are aspects of the business's culture that may be reflected in the question or tasking.

There are two basic categories of questions, determining what should be shared and determining the best route for security. Although closely related and highly interdependent, these

[3] Peter H Daly, "Soldiers, Constables, Bankers and Merchants Managing National security risks in the Cyber Era", Draft, 22 Nov 1999, PIRP, page 32

[4] *Joint Vision 2010*, Chairman Joint Chiefs of Staff, access from http://www.dtic.mil/jv2010/jv2010.pdf, 7 Dec 99, 9:52am, page 2

[5] *C4I for the Warrior*, The Joint Staff, Director, Command, Control, Communications, and Computer Systems, undated, JCS/J6I, page 1

[6] Adaptation from Charles Popper's, "A Holistic Framework for IT Governance", January 2000, Harvard's Program On Information Resources Policy (PIRP), copyright 2000, chapter 1, page 1

[7] Dr James J Hearn, Former Deputy Director of NSA, 13 Dec 99 interview with the author

two categories of questions present vastly different problem sets. In attempting to address both aspects of the information sharing and security in one question or tasking, organizations may find themselves with an overwhelmingly complex task. This complexity comes from the underlying differences in the basic objectives of sharing and security, as well as the stakeholders and stakes involved. Specifically, the basic motivation behind information sharing is adding value, while the basic motivation of security is avoiding losses. On the question of sharing, the basic objective is to maximize information value to the business through its dissemination. On the question of security, the basic objective is to minimize liabilities by addressing threats and vulnerabilities to the information through its protection and safeguarding.

As a common rule, addressing the question of which information to share first will provide a clearer picture for addressing how to best secure the environment, as most would not argue that knowing what you are sharing can be a driving factor in determining how to secure the environment. However, there may be things that you will share only if you can share them safely, therefore the dependence also flows the other direction. The important idea is to ensure that questions clearly reflect which aspect of information sharing and security is being addressed.

The wording of the question or task can imply whether the emphasis of the organization is primarily to share or secure its information. Is the organization's approach to sharing and security permissive or restrictive in nature? The difference can be as minor looking as asking what information can be shared versus what information must be shared. In a permissive information sharing environment, information is shared unless there is a reason not to. In the restrictive environment, information is shared only when there is a reason to. In a permissive security environment, the default is to not secure information. In a restrictive security environment, the default is to secure the information. Which formulation is correct will be a dynamic of the business's culture.

Just as organizational culture is reflected in the information sharing and security objectives and success criteria, when ever a cultural aspect of the organization must be changed to accommodate a new approach to information sharing and security, steps may be needed to account for the cultural shifts. By linking information sharing and security approach to the culture and environment of the organization, we are more likely to get an information sharing and security approach that make sense to the people, is more relevant to their jobs, and adds value to their work.

In our two samples, the role of business culture varies greatly. In the GCCS environment, the culture is relatively homogenous with a common approach to security and relationships that are established and often long standing. In the PDD sample, the cultures of the various entities is vastly diverse with different approaches and philosophies about security, and most relationships are not yet defined or established. In both cases, highlighting cultural considerations (Tables 1 & 2) is beneficial.

For the PDD scenario, both PDD 62 and PDD 63 call for the federal government entities, in particular DOD and the intelligence communities, to share information with each other as well as with National, State, and Local Law Enforcement and Industry. One example of the cultural differences in the entities is the classification of the President's Commission on Critical Infrastructure Protection (PCCIP) vulnerability findings. From the military perspective, taking steps to prevent the unveiling of our vulnerabilities is a logical and necessary step. To the private sector, this action can be seen as comparable to taking your car to the mechanic and having them tell you that your car is in desperate need of repair, that they are not going to tell you what is wrong, and they are not going to fix it – but, if you want to fix it they may help you fix problems you find!

Table 1 - PDD Entity Cultures Highlights

Entity	Sharing and Security Environment (Internal and External)	Cultural Highlights
Federal Government • Department of Commerce • Department of State	• Default is to share information • Default is not to secure information	• National Interest Focus • Public Confidence Paramount to Success • Statutes and Public Good criteria for action
Department of Defense	• Default is to share information • Default is not to secure information • Default is to secure vulnerability information	• National Security Focus • Information Used to Fight and Win Wars • Jurisdiction is Outside US • Security Requirements established in Statute, policy and doctrine • Public Confidence Paramount to Success • Protection of Nation and way of life as a whole criterion for action
National Intelligence Agencies	• Default is not to share information - Information dissemination based upon need to know • Default is to secure information	• National Security Focus • Jurisdiction is Non-US Only • By Statute, Highly Protective of Source and Methods • Public Confidence Paramount to Success • Providing strategic and tactical decision support to President, Secretary of Defense and National Security Advisor motivation for action
National Law Enforcement	• Default is not to share information • Default is to protect information	• Capture and Conviction of Federal Criminals Focus • Jurisdiction is Federal and International Only (Statutes and Area) • Violation of Federal Laws motivation for action
State Law Enforcement	• Default is not to share information • Default is to protect information	• Capture and Conviction of State Criminals Focus • Jurisdiction is within State Only (Statutes and Area) • Security approaches and emphasis controlled by individual states. • Violation of State laws motivation for action
Local Law Enforcement	• Default is not to share information • Default is to protect information	• Capture and Conviction of Local Criminals Focus • Jurisdiction is Local Only (Statutes and Area) • Security approaches and emphasis controlled by individual departments. • Violation of Local Laws and Ordinances motivation for action
Industry (Banking, Communications, Transportation)	• Default is not to share information • Default is to protect information	• Business Value Focus • National and International Interests • Customer Confidence Paramount • Security approaches and emphasis controlled by individual corporations. • Does not inherently trust government with data • Profit and losses motivation for action

What Table 1 highlights is that the entities involved have different approaches to security, different uses for the information, different methods of collecting their data, and different motivations, interests and goals overall. This is a strong indication of the complexity of the problem being faced by those charged with carrying out the PDDs. But it is also an indication of the level of compromise, innovation, and cooperation that will be needed to make a solution possible.

For the purposes of this example, the GCCS scenario is treated as a single cultural environment; therefore, the cultural issues enter the equation from a different perspective. In general terms, DOD is a permissive sharing and security environment. However, the sample scenario is dealing with the classified environments, making the default immaterial. What is important is trying to capture what some of the key enablers and obstacles about the culture that may impact the sharing and security approach. In dealing with the issue of separate LANs being maintained for separate security classifications, as presented in the GCCS sample scenario, some of the cultural aspects are presented below.

Table 2 - Cultural Highlights for GCCS Communication/Computer Environment

Entity	Sharing and Security Environment	Cultural Highlights
War fighters	• Information spread across several computer systems at varying security levels. Voice, hardcopy, imaged, and signal data often handled simultaneously. • Established policies, procedures, and guidelines for securing and sharing information.	• Primary producer and consumer of information. • In peace time, heavy reliance and close adherence to security policies, procedures, and guidance • In war or times of crisis, security constraints may be temporarily out weighed by mission requirements • Traditionally, senior management minimally involved in security environment decisions. Heavy reliance on technical and security communities to establish, monitor, and maintain the security environment • Often see security as a cost of doing business, not as a business enabler • Deployed Warfighter is predominately dependent on SECRET and UNCLASSIFIED access
Intelligence Community	• Established and strong adherence to policies, procedures, and guidelines for securing and sharing intelligence information. • Secure is default.	• Role is to develop and provide intelligence information. Secure is default. • Sees security as paramount to mission success, particularly when pertaining to protection of sources and methods. • Senior management involvement in security environment. • Analysts operate predominately in compartmented-mode security environment
Information Infrastructure Support Personnel	Established and strong adherence to policies, procedures, and guidelines for managing and maintaining information infrastructure and technical Automated Data Processing (ADP) security posture	• Role is to provide information infrastructure, serve as custodian for information on that infrastructure, and provide technical expertise. • Overall responsibility for security of communications and computer systems.
National Security Agency/ Cen tral Security Service (NSA/CSS)[8]	• Established and strong adherence to policies, procedures, and guidelines for securing and sharing intelligence information. • Secure is default.	• Role is provider of foreign intelligence information and computer security expertise to DoD; serve as security experts, providing threat and vulnerability information as well as monitoring and assessing security posture of information infrastructure.

[8] National Security Agency information consolidated from http://www.nsa.gov web site. Articles included the National Cryptology Strategy for the 21st Century, the NSA mission, About NSA, and NSA FAQ pieces downloaded on 10 Mar 2000.

Chapter 3 – Information Sharing and Security Objectives

Balancing information sharing and security can be broken into three basic tasks: 1) determining the purpose of information sharing and security in the organization (objectives), 2) developing an approach, 3) assessing, managing, and adapting to the impacts of the approach. This paper does not present the process and procedures for accomplishing each of these tasks. What this paper aims to provide is ideas and insights for adjusting and refining those processes already in place in the organization to bring them into a more business-oriented or operational focus.

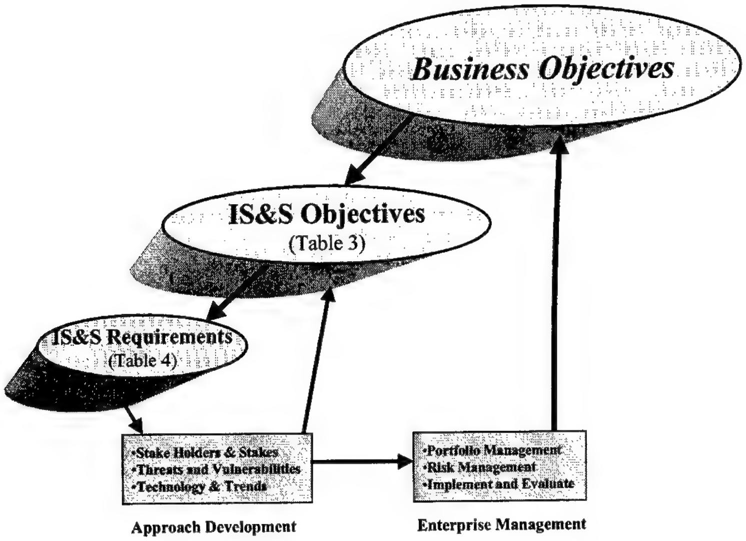


Figure 4 - IS&S: Developing Objectives and Requirements

The relationship of business objectives to information sharing and security objectives – a holistic approach to information sharing and security.

> *"We are not in the business of protecting information. We only protect information insofar as it supports the business needs and requirements of our company."*
> – Senior security manager at a major electric utility.[9]
> –

Most organizations will initiate their information sharing and security approach by establishing objectives, from the perspective of what we want to accomplish and what the expected results will be. Information sharing and security requirements may be operationally, politically, or legally rooted, and cost money, require resources, and impact virtually all aspects of a business: its people, processes, procedures, technology, and partners. Given this, what should be the basis for the information sharing and security objectives? Typically, one begins

[9] GAO Executive Guide, "Information Security Management: Learning from Leading Organizations," May 1998, GAO/AIMD-98-68 Information Security Management, page 21

with the business strategy of the enterprise, identifying the main value-adding activities and strategies to enhance. [10,11,12] However, some organizations allow information sharing and security objectives to be based upon and driven by the security community's or the information management and infrastructure community's objectives.

A major complaint is that security is impeding operational effectiveness or the ability to conduct business because it is thwarting the ability to share information when there is no compelling security concern that outweighs the operational concern in a business sense[13]. This could be a result of basing information sharing and security objectives on objectives that are not focused on the operational side of the business. The information infrastructure support, information management, and security communities focus on specific support aspect for the operational side of the business. Because of the natural tendencies of groups, one would assume that their objectives, solutions, and metrics make sense and fit nicely into their community's efforts, but there are no assurances that they would not align at all with the overall business approach. Because of the difference in emphasis and focus, the security, information infrastructure, and information management communities may not be the best sources for information sharing and security objectives. Or would the information sharing and security objectives more properly reflect the organization's overall objectives if they were derived from the overall business objectives? By linking information sharing and security objectives to business objectives, we get information sharing and security objectives that are more likely to be relevant to overall business direction and highlight how they can add value to the business.

But how will we know when, or to what degree, we have achieved the information sharing and security objectives? As the information and security objectives are developed, developing the criteria by which achieving the objective will be measured often helps clarify the objective and quantify expectations. "Sufficiently rapidly, sufficiently accurately, and sufficiently economically", was the terminology used by Claude Shannon in his 1948 book, "Mathematical Theory of Communication."[14] But the most frequent interpretation of these criteria is measuring the technical aspects of the communications, failing to address success or failure from the business perspective. By adding business oriented success criteria to the objectives, emphasis and clarity are enhanced by focusing back on the business value added expectations of information sharing and security.

Whether an organization uses measures of performance (MOPS), performance measures, metrics, or criteria for success (CFS), there is benefit to relating the measures and the subsequent analysis to the information sharing and security approach's impact on the organization's business objectives. For example, the military goes through a process called 'security accreditations' that verifies the security environment for a classified system. However, doing an accreditation only assesses the security level of a particular environment, it would not reveal if the security constraints are bringing business operations to a grinding halt. Likewise, monitoring employee compliance with security guidance does not provide information on the guidance's impact on the timely information flow.

[10] GAO Executive Guide, "Information Security Management: Learning from Leading Organizations," May 1998, GAO/AIMD-98-68 Information Security Management, page 24

[11] Charles Popper, "A Holistic Framework for IT Governance", January 2000, Harvard's Program On Information Resources Policy (PIRP), copyright 2000, chapter 2, para 2.1.2, and chapter four

[12] GAO Executive Guide, "Information Security Management: Learning from Leading Organizations," May 1998, GAO/AIMD-98-68 Information Security Management, page 24

[13] Colonel Gordon Thigpen, Director, Current Situation Operations Division (CSOD), JCS/J3, 15 December 1999 interview with the author

[14] Irwin Lebow, "Understanding Digital Transmission and Recording", IEEE Press, 1998, chapter 5, page 75

If there are expectations that a new information sharing and security approach will act as a business enabler[15], success criteria can be used to document such expectations including building customer confidence, increasing user trust, increasing reliability, or increasing awareness of business objectives by highlighting to employees what the business considers important.

Table 3 provides a fairly simple conceptual tool for presenting sharing and security objective information. The essence of Table 3 is to summarize the sharing and security objectives as they relate to the overall business objectives. In addition, the chart also depicts the current status, from a business value perspective, of progress towards the objective. When appropriate, recommended actions can be depicted. The chart assumes that success criteria are presented as part of the objectives. Such a summary presentation can give senior management a quick overview of the direction, status, and benefits of the sharing and security effort in a manner that is related to their overall business concerns.

Table 3 - Sample Information Sharing &Security (IS&S) Objectives

Business Objectives	**Sharing and Security Role/Objectives**	**Business Value Based Assessment/ Recommendation**
1) Increased Sales 2) Lower Production Costs Per Item 3) Increased Market Share	1) Enable achievement of business objectives by providing an economically, technically, and critical resource feasible, information sharing environment that is sufficiently secure and enhances operating efficiency. Measures of Performance: a) Enable achievement of business objectives i) Sufficiently flexible to adapt to and adopt to new business practices ii) Enable consumers to access the data they need when they need it easily and quickly b) Sufficiently Secure i) Acceptable vulnerability mitigation level against information attacks ii) Acceptable vulnerability mitigation level against information espionage iii) Acceptable vulnerability mitigation level inadvertent internal information quality compromise or exposure iv) Acceptable levels of information sharing and security training and awareness c) Economically feasible. Within cost constraints d) Technically feasible. Acceptable risk to availability of needed security technology and the availability of required skill set support personnel e) Critical resource feasible. Achievable and supportable with the ADP support personnel, bandwidth, and consumer personnel available	*At the beginning of the IS&S approach development process, use this area to highlight how well the current environment meets the objectives.* *Once the process is completed, recommendations and justifications can be highlighted here*

Once the objectives have been captured, identifying the associated information that must be shared, secured or securely shared enumerates the requirements for the IS&S approach. Again, identifying the business value when capturing sharing and security requirements may help in understanding and prioritizing aspects of the approach. A chart like table 4, more so than other charts, may need to be constantly revisited, updated, and refined as information on culture, stake holders, trends, and vulnerabilities, which are discussed in the following sections, come to light.

[15] GAO Executive Guide, "Information Security Management: Learning from Leading Organizations," May 1998, GAO/AIMD-98-68 Information Security Management, page 23

Table 4 - Sample Information Product Requirements

IS&S Objective	Information or Information Product[16]	Sharing Opportunities	Security Requirements	Issues/ Recommendations

Using the approach portrayed in Table 3 for the PDD scenario, the objectives pertaining to the sharing of information between the federal, state, and local agencies with industry are briefly summarized below.

Table 5 – Summarizing PDD Sharing and Security Objectives

Business Objective	Sharing Role/Objectives	Security Role/Objectives	Business Value Based Assessment/ Recommendation
Protection of National Interests by deterring attacks, protecting, responding, and recovering	1. Threat Intelligence information readily available to those that need it 2. Attack Warning generated and disseminated in timely enough fashion to be effective 3. Attack detection occurs with sufficient accuracy, including timeliness, to enable creditable response 4. Attack Information shared in sufficient quantity and quality to enable the various organization to accomplish their roles and missions	5. Protection of Organizational Resources; 6. Protect Public's Confidence in overall Infrastructure as well as individual participants 7. Deter attacks	*Environment yet to be established*
Proper Response to Attacks	8. Investigation Information of sufficient quality, including timeliness, available to determine scale of attack, identify attacker(s) and support proper law enforcement or military response	9. Adherence to Privacy and other information statues and policies 10. Investigation and pursuit of attackers should not unduly impact victims, or make more victims	*Environment yet to be established*
Public Confidence	11. Enhance public awareness and confidence in information infrastructure protection 12. Increase private sector participation as information infrastructure protection partners with government	13. Avoid 'Big Brother' Syndrome 14. Government awareness and priority for protection of customer confidence, business reputations, intellectual property and other private sensitivities when accepting and using infrastructure protection information from private sources	"Therefore, the common interest in anticipating and avoiding events that put critical public confidence at risk may well be the primary motivating force for government and major business sectors to rethink their respective compartmentalized perceptions of risk, and to undertake to restyle the traditional government-business national security relationship so that risks may be jointly determined."[17]
Conservation and effective/efficient use of critical resources (i.e. analysts, computer techies, LEA as well as bandwidth and computing power)	15. Alignment of analytical processes to allow sharing of information collection and analysis, allowing for reduction in similar or duplicative efforts 16. Effective information sharing to reduce number of duplicated efforts	17. Sharing and Analysis cannot undermine the security and integrity of the various organizational operations	

[16] For additional discussion on information products and other terms, refer to the 'Talking Eye-to-eye' Appendix to this document.

[17] Peter H Daly, "Soldiers, Constables, Bankers and Merchants Managing National security risks in the Cyber Era", Draft, 22 Nov 1999, PIRP, page 31

The business objectives outlined in Table 5 were derived from reading PDD 63, the White House's White Paper on PDD-63[18] and the National Plan for Information Systems Protection, version 1.0[19], and discussions with General (ret) R Thomas Marsh. What would the difference be in private sector support if the earlier recommendations of this paper regarding culture and wording were applied and these objectives were presented as for example:

- Protection of Investment;
- Ensuring proper response while protecting privacy and privileged information;
- Protection of Reputations and Customer Confidence; and
- Affordable and Feasible?

However, given the objectives as given in the chart, what are the information products that will be needed to accomplish these objectives?

Table 6 - IS&S Information Product Requirements for PDD Scenario

IS&S Objective	Information	Sharing Opportunities	Security Requirements	Issues/ Recommendations
Threat Intelligence information readily available to those that need it	Threat Intelligence			
Attack Warning generated and disseminated in timely enough fashion to be effective	Attack Warning Information			
Attack detection occurs with sufficient accuracy, including timeliness, to enable creditable response	Attack Detection information			
Attack Information shared in sufficient quantity and quality to enable the various organization to accomplish their roles and missions	Attack Characteristics Information			
Protection of Organizational Resources				
Protect Public's Confidence in overall Infrastructure as well as individual participants				
Deter attacks				
Investigation Information of sufficient quality, including timeliness, available to determine scale of attack, identify attacker(s) and support proper law enforcement or military response				
Adherence to Privacy and other information statues and policies				
Investigation and pursuit of attackers should not unduly impact victims, or make more victims				

[18] WHITE PAPER The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, 22 May 1998, The White House, downloaded from http://www.whitehouse.gov/WH/EOP/NSC/html/nschome.html#doc on 2 September 1999

[19] National Plan for Information Systems Protection: Defending America's Cyberspace– An Invitation to Dialogue, version 1.0, The White House, January 2000, downloaded from http://www.whitehouse.gov/WH/EOP/NSC/html/nschome.html#doc in January 2000

In many instances, stakeholders have widely varying objectives for information sharing and security relevant to a particular business objective. In such cases, developing a chart such as Table 7, which capturing stake holders’ objectives by business objectives, helps to ensure that the various perspectives of the issues are identified. This information can then be summarized and highlighted in a Table 5-style portrayal. Capturing the information in the context of Stakeholders and stakes is discussed further in the chapter 4.

Table 7 – Model Information Sharing & Security (IS&S) Objectives by Stakeholders

Business objective	**Stakeholder/stake**	**Information Sharing Objectives**	**Information Security Objectives**	**Current Business Value Assessment**	**Business Value Assessment of Proposed Changes**
Objective 1				*How well does the current environment meet the objective?*	*Assessment of recommended changes*
	Information Consumers				
	Information Providers				
	Information Protectors				
	Information Custodians				
Objective 2					
	Information Consumers				
	Information Providers				
	Information Protectors				
	Information Custodians				
. . .	. . .	. . .			

As an example, military guidance[20] and direction[21] sets objectives of Dominant Battle Space Awareness and Information Superiority. Focusing on the question of multiple networks for multiple levels of security, the war fighters' information sharing and security objectives may include being able to access all their data sources from a single workstation, while the intelligence community's objective is to ensure timely and accurate intelligence information is available to the war fighter. Some of the stakeholders and their IS&S objectives for the of Dominant Battle Space Awareness and Information Superiority business objectives are captured in Table 8.

Table 8 - GCCS Single Workstation Access Objective

Business objective	**Stakeholder/stake**	**Information Sharing Objectives**	**Information Security Objectives**	**Current Business Value Assessment**	**Business Value Assessment of Proposed Changes**
Dominant Battle Space Awareness And *Information Superiority*		*Common to all stake holders* *- WIN!* *- save money and resources*			
	War fighter/ Business Critical	1. Single workstation access to information. 2. – Improve war fighter efficiency and effectiveness	3. Protection of National Security Information, plans, and operations	The separate, disjoint realization is significantly impacting information accessibility, availability, and reliability. Accessibility and availability cost the enterprise staff hours and decision accuracy as people have to physically move from workstation to workstation to collect, analysis, assimilate, cross check, and disseminate information. The reliability aspect stems from information being copied to various networks for accessibility reasons, where the information subsequently gets out of synchronization with the source information thereby jeopardizing the quality and value of the information and subsequent decisions.	
	Intelligence Community/ Business Critical	4. Getting timely accurate intelligence to the war fighter	5. Protection of Sources and Methods		
	National Security Agency – CSS /Business support		6. Secure Information Infrastructure Operations		
	Joint Staff/ Business support				
	DISA and ADP support personnel/ Business support, critical resource constrained	7. Optimize bandwidth and computational resources to ensure ability to meet war fighter needs	8. Provide a secure information infrastructure		
. . .	. . .	. . .			

[20] Joint Vision 2010, Chairman Joint Chiefs of Staff, access from http://www.dtic.mil/jv2010/jv2010.pdf, 7 Dec 99, 9:52am

[21] C4I for the Warrior, "*A Joint Vision for C4I Interoperability*", Joint Staff J6, January 1998, page 1

Table 9 - Example of Information Requirements for GCCS Scenario

IS&S Objective	Information	Sharing Opportunities	Security Requirements	Issues/ Recommendations
- Single workstation access to information. - Improve war fighter efficiency and effectiveness	War Fighter Information	Access to war fighter data from multiple classification levels from a single workstation	Deployed Troops operate at predominately SECRET and UNCLASSIFIED - Security Level for access is determined by the security clearance and need to know permissions of the person, the security level of the physical environment, the security level of the workstation and the security level of the supporting communications	
- Getting timely accurate intelligence to the war fighter - Protection of Sources and Methods	Intelligence Products			
Optimize bandwidth and computational resources to ensure ability to meet war fighter needs	All			
Protection of National Security Information, plans, and operations	All			
Secure Information Infrastructure Operations	All	- Security Posture Data - Security Effectiveness Data - Security Efficiency Data	Trained and Cleared Support and Operational Personnel	
Provide a secure information infrastructure	Defense in Depth Information		Trained and Cleared Support and developmental Personnel	

Chapter 4 – What Plays a Role

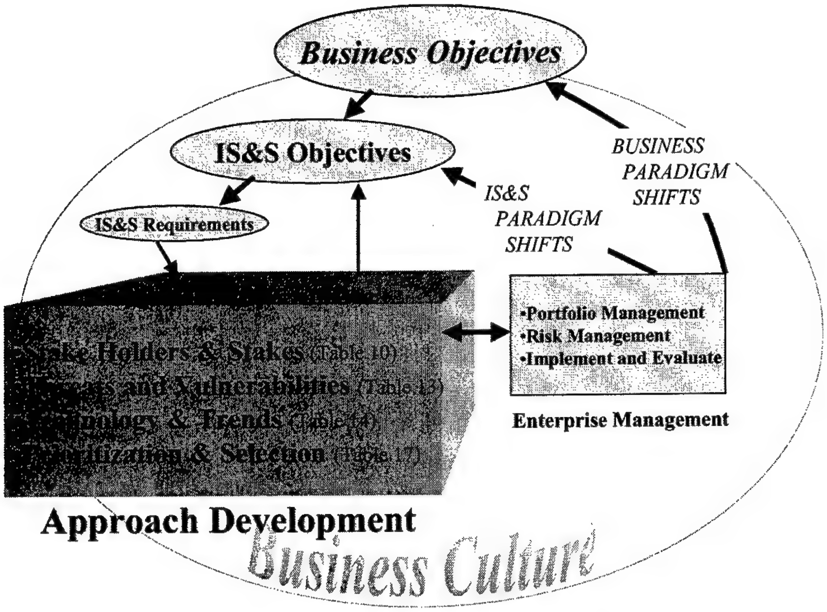


Figure 5 - Identifying the Influences for Information Sharing & Security Approach

Whether it is a new organization creating its security and sharing approach, or an existing organization looking at specific issues, the number of factors and options to consider may seem infinite. Therefore, it may be extremely helpful to start by capturing and understanding a number of those factors influencing the basic questions of why we share information and why we secure information. Examining and understanding stakeholders and what is at stake helps to identify, weigh, and prioritize issues and options within the balancing act. Identifying the threats and vulnerabilities tells us the specific questions to be addressed. The double-edged sword of technology and the dynamics of the business and the information worlds simultaneously bound the realm of possibilities, provide possible answers, and raise new questions.

1. The Role of the Stake holders and Their Stakes

> *"The advent of the information age will require, as never before, that we take a wider perspective and avoid stovepipes that blind us to changes taking place outside our own sphere of direct responsibility.*[22] *"*

Who has a vested interest in an organization's approach to security? Traditionally, stakeholders have been categorized as consumers and providers of information, and, in some instances, its protectors (see 'Talking Eye-to-eye' Appendix for more detailed discussion of

[22] Andrew W Marshall, "Strategic Appraisal: The Changing Role of Information in Warfare", Forward, RAND, Project Air Force, @1999, RAND, page 2

terms). With the move into global interconnection and interdependence, the list of traditional stakeholders is expanding to include global consumers, providers, and protectors of information. In addition, the information explosion is bringing a the proliferation of copied data and creating a global shortage of information infrastructure technical support people, making it important to identify the sources and owners of information, and give greater consideration to the information infrastructure developers, maintainers and managers.

As interconnection increases, within an organization or globally, the complexity of the stake holders and stake picture increases dramatically. Decisions on sharing information must consider not only the immediate environment, but also the environment to which the information is being passed to or from. As information is passed and duplicated, what happens to the vested interests of the original data owner? When information is duplicated, who is the owner of the new information source? Who is responsible for security of that information source? Who is liable for that information source? As we secure our environment, does our approach to security need to allow for external data sources? For external data consumers? How do the laws and regulations on technology sharing apply to an international corporation sharing data across national boundaries? What kind of burden does our security approach place on our customers? If we share information with a business partner, with whom may they share the information? If we accept information from someone, do we accept a liability for that information? What do they expect in return?

The U.S. military places great emphasis, in both policy and practice, on being as forthcoming with the news media as possible on military operations. Therefore, with the obvious restriction of not discussing operational details that will help the enemy, the U.S. Military has traditionally allowed soldiers, airmen, and sailors to be interviewed and shown performing their war time tasks. However, in the globally connected information age, the military found there was a new stakeholder in the equation, the military members and their families. During the Kosovo crises, a routine interview with an air crew, where the pilots' names were given, resulted in hate mail and death threats to the military member's home after Serbian supporters were able to look up the needed information about the pilots on the internet.[23]

Another important aspect of the example is that it also illustrates how culture once again can factor into information sharing and security. One may be tempted to argue that, from the overall military perspective, the threats to a single or limited number of aircrew members and their families is of little significance. However, even placing the impact on the war fighter morale, etc. aside, given the precious life culture of Americans, few in the US or military would see the harming, either physical or psychological, of the war fighter's family as acceptable.

A commonly accepted paradigm is where the business community sees security as a cost of doing business over which they relatively little control. In fact, the business community has become so accepting of the saying 'security is a cost of doing business' that it has resulted in: 1) security being seen as separate from core operations including establishing separate organizations to handle security; 2) security being treated as an 'add on' rather than 'built into' our information systems; 3) a communication failure between operators, information providers, and information protectors; and 4) lethargy about business constraints in the name of security. But basing the information sharing and security objectives on the security community's objectives implies that security is the dominant factor in the sharing and security balance, propagating the security is a cost of doing business paradigms. While there may be merit to having a separate pool of security expertise, should they be the group making the final call between business and security trade-offs? With the exploding dependencies on information and information technology, continuing to foster these paradigms, particularly on the communications and computer side, may no longer be acceptable, desirable, or feasible.

[23] Lt Gen John Woodward, JCS/J6, 14 Dec 1999 interview with the author

One approach to countering this paradigm is to have key stakeholders actively involved in identifying and assessing vulnerabilities, developing and implementing the security architecture, and executing the security realization. Information consumers and providers not only have the largest business value stake in the information vulnerabilities, it will also be their business processes most affected by the security realization, and their people will carry the bulk of the load in executing the realization. Finally, it will be the business environment that will be affected by the efforts traded away in order to accomplish information sharing and security

In addition to the information consumers and providers, the information infrastructure operations and maintenance communities may also have a large stake in the realm of resources needed to support various sharing and security approaches. Since these represent recurring, long-term commitments, the cost and availability of these increasingly sparse skill sets directly impact the economic and technical feasibility of approaches.

Once again comes the question of information ownership, often called the information originator by the intelligence community. What should be the role of the information owner in establishing whom their information will be shared with? What should be the role of the information owner in setting security requirements and verifying security approaches? And most important, who is the information owner? If an organization a copies a database onto their network, who owns the information in the duplicate database? Is the owner the source of the information, the holder of the information, or the provider of the information? If the information source is to remain the information's owner, will the receiving organization allow the source to dictate what the receiving organization can and can not do with the information? If the information owner is external to the organization, who represents the information owner's interests? If our organization passes information to outside entities, what will be our position on these questions? The answers to these questions are not straightforward.

For instance, when a consumer gives an e-commerce web site their credit card information, who owns that information? What are the rights and obligations of the each of the parties? What are the rules for subsequently sharing that information? Or when sensitive intelligence information is duplicated on to military networks to allow faster access, who makes the call that the security environment on the military network is adequate? Who is responsible if the information is compromised? If the information is out of date? If the information is corrupted? And if commercial entities share information on security intruders and cyber attacks with government agencies, who owns that information and determines what can be done with it?

In some instances, statutes and regulations outline the answers to these questions, but the culture and dynamics of the particular business will also greatly influence the answer. If a common understanding of the organizations' perceptions of ownership is missing, key decisions may be faulty because they are based upon bad assumptions. Therefore, the benefits of establishing guidelines that address these information ownership questions early can be enormous, even if such guidelines need to be amended or exceptions granted as the process evolves. Following this by assigning or acknowledging the owner of information, and clearly stating what ownership entails, can also serve to prevent confusion and misunderstandings later.

Devising a general model that addresses these issues for all, or even most, situations is a daunting, if not impossible, task. However, one vital step that can be taken is to identify the stakeholders and their stakes. Presenting decision-makers with an organized portrayal of the major players and their interests can help frame the issues, even if the answer is not completely clear. Quantifying the stakes in terms of resources, productivity, and business value will help clarify and prioritize the stakes. In addition, stakes can also be incorporated into success criteria, once again highlighting expectations.

Below is a simple example. Suppose a 'Feline Stories' web site is being expanded to sell books on cats. Customers are provided merchandise descriptions and pricing information, and use their credit cards to submit orders. The site automatically orders the books from the wholesalers. The site owner pays the vendor and makes a charge to the customer's credit card for the books, adding a small surcharge and taxes. Customer information is retained to ease subsequent purchases. Table 10 provides a sample set of the stakeholders and their stakes for this example.

Table 10 - Stakeholders and Stakes for Feline Stories E-commerce

Stakeholder types	Sample Stakeholders	Stakes in sharing	Stakes in security	Contentions	Recommendations
Consumer	Potential Customers (descriptions and pricing information)	Easy access to book information.	Trust in book descriptions and prices.	The more secure the web site, the less user friendly it may be if it requires passwords, special client software, etc	Make site as secure as possible without requiring specialized client software or passwords for read-only access to site
	Wholesalers (ordering and shipping information)	Ability to fill orders properly and make money	Trust in order and shipping information		
	Accounting department (ordering and billing information)	Ability to manage revenues, pay taxes, pay salaries, ensure orders are filled as ordered			
	Future Business Department (sales information)	Ability to expand business by doing analysis on buying trends			
	Infrastructure Support (number of site users, volume of orders, sensitivity of information provided)	Maintaining optimum infrastructure configuration and efficient operations. Ability to trouble shoot and recover from problems	Web server sizing and security		
Providers	Customers		Ease of order entry, Protection of Credit Card Data from Credit card fraud, disclosure of credit information, etc		
	Wholesalers		Customer orders and customer confidence		
Owners					
Protectors	Infrastructure Support		Resource required to accomplish security approach		
	Business		Legal privacy requirements[24], Business relationships – Reputation and customer satisfaction		

Collecting and charting the stakes of the stakeholders helps to ensure that the many sides of the sharing and security issue are recognized and addressed. Charting the information, as in Table 11, also eases the process of identifying conflicts within and between stakeholders and documenting recommended remedies. This allows the stakeholders and managers to better visualize the impacts of recommendations and the trade-off considered in the decisions.

Just as important is recognizing the potential consequences of each security approach on each stakeholder. Pulling your finger out of the dike and running may only get you wet, but it may ultimately flood the village. Another emerging aspect of the global market coupling is the far-reaching impacts one entity can have on others. Capturing each stakeholder's contributions and requirements can help in achieving a fuller appreciation and understanding of the stakes and impacts of decisions. There are some items clearly missing from the following chart. Who will pay for the information sharing and security infrastructure for PDD 62 and 63? Who is responsible for the overall success of program? And, who determines what is secure enough?

[24] Under stakes, a lot of information on legal requirements is outlined on pages 10 and 11 of GAO Executive Guide, "Information Security Management: Learning from Leading Organizations," May 1998, GAO/AIMD-98-68 Information Security Management.

These items are missing because they are currently unanswered. Peter Daly does an excellent job weighing the question of “who will pay for the security”, “who will choose the response?” and “who will assure readiness?” in his paper entitled, “Soldiers, Constables, Bankers and Merchants Managing National security risks in the Cyber Era.”[25]

Table 11 Summary: Sharing and Security Stakes for PDD Attack Detection and Response

Stake Holder Class	Stakeholder	Sharing Stake	Security Stake	Contention Assessment
Information Consumer	1) Federal Government 2) National, State and Local Law Enforcement 3) Critical Infrastructure Assurance Office (CIAO) /Computer Emergency Response Team (CERT) 4) Other Sites that are vulnerable to similar attack	1) Ability to determine if national attack 2) Ability to pursue and prosecute criminals 3) Situational Awareness 4) Situational Awareness	1) Rapid response to national security threat 2) Deterrence for additional attacks 3) Ability to coordinate wide-spread attack response 4) Ability to preempt attack on their site	• Federal gov’t ability to monitor/respond and the ‘Big Brother syndrome’ • National response versus individual (or limited number of) corporation’s reputation/ customer confidence • Advertising success for a terrorist versus notifying public of threat/ vulnerability • “The one common denominator is public confidence. Both government and business derive viability from it, view it as a critical resource, and – importantly – will go to great lengths to retain it.[26]”
Information Provider	5) Site(s) being attacked	5) Call for assistance, ability to warn others	5) Loss of customer confidence if attack information revealed by government	• Warning other sites versus customer confidence • Getting help versus customer confidence
Information Protector	6) Security Software Vendor for Attacked Site(s) 7) Attack Response Support for attacked Site(s)	6) Loss of Customer confidence in product 7) Ability to receive counter measure in timely fashion	6) Ability to develop/ deploy countermeasure 7) Jobs at stake?	• Vulnerability awareness for customers versus vulnerability awareness for attackers •
Information Custodian	8) ADP support staff	8) Ability to recover from attack	8) Staff hours used in responding and recovering from attack	• Staff hours to participate in national security program, including training, versus staff hours to support direct customer base

[25] Peter H Daly, “Soldiers, Constables, Bankers and Merchants Managing National security risks in the Cyber Era”, Draft, 22 Nov 1999, PIRP, pages 32-35

[26] Peter H Daly, “Soldiers, Constables, Bankers and Merchants Managing National security risks in the Cyber Era”, Draft, 22 Nov 1999, PIRP, page 30

Initially, it may be beneficial to sort and examine the stakes and conflicts by the various information products. This more detailed view can allow stakes to be prioritized by information product importance, and can assist in highlighting particular 'problem' products, possibly allowing for recommended information product changes or recommendations for certain stake holders to use different products that better suit their needs. See the Talking Eye-to-Eye appendix of this paper for explanations of information products and other terms.

Table 12 - Across GCCS Information Products: Sharing and Security Stakes Details

Information Product	Stake Holder Class	Stakeholder	Sharing Stake	Security Stake	Conflicts
War Plans	**Information Consumer**	Field Units, transportation providers, deploying forces, Task Force Commander and staff	1) Ability to get the right forces to the right places at the right time to win the war. 2) Ability to communicate plan and execution decisions in a timely and reliable greatly manner to effectively and efficiently carry out plan	1) Surprise; do not want the enemy to know when, where, and who of our plan. Must provide proper level of security for 2 different security levels of plans during execution 2) Time and expertise to execute the sharing and security approach 3) adherence to NDP-1 and other statutory requirements for sharing classified and privacy data with allies and coalition partners	The war fighting community concurs that the separate, disjoint realization is significantly impacting information accessibility, availability, and reliability. Accessibility and availability cost the enterprise staff hours and decision accuracy as people have to physically move from workstation to workstation to collect, analysis, assimilate, cross check, and disseminate information. The reliability aspect stems from information being copied to various networks for accessibility reasons, where the information subsequently gets out of synchronization with the source information thereby jeopardizing the quality and value of the information and subsequent decisions[27]
	Information Provider	Planning staffs, transportation managers, deploying units	Timely and realistic Supportability and capability feedback critical to planning.	Must provide for security of 3 different level of plans during plan development	
	Information Protector	National Security Agency, Software Vendors, DISA, GCCS SWG[28]	Financial well being of Secure Software Vendors and security Technology markets	Enforcement of National Security Regulations and Guidance for handling and processing classified information	
	Information Custodian	ADP Support Staff	1) People, tools, time and money to implement and operate sharing realization. 2) Enforcement of National Disclosure Policy (NDP) 1 (NDP-1). 3) Determination by NDP Committee (NDPC) of what information can be released or disclosed to allies and coalition partners	People, tools, time and money to implement and operate security realization	

[27] Colonel Gordon Thigpen, Director, Current Situation Operations Division (CSOD), JCS/J3, 15 December 1999 interview with the author

[28] GCCS SWG is GCCS Security Working Group chaired by Joint Staff with representatives from all nine war fighting commands

2. Threats, Vulnerabilities, and Mitigation

> *"Experience indicates that the current vulnerabilities may not persist. Little attention has been paid to building defenses until now. The technology is changing rapidly, and information systems continue to evolve as they keep up with these changes.[29]"*

The information age has not only brought disruptive technology for business[30], but it has also been a disruptive technology for information security. The Internet and interconnections change not only the number, but also the type of threats, and the potential damage they may cause. In e-commerce, an entire venture can be lost if the customer base loses confidence in the site's security. The damage of a site being 'hacked' may not be the information lost to the hacker, but rather the loss of business reputation because your site was hacked. Therefore, as security threat assessments are conducted, business value based damage assessments may need to be developed to augment the technical damage potential assessment.

Sharing and security approaches, like operational implementations, must be flexible/adaptable to keep pace with the changing world, technology, and evolving threats. In some areas, especially in commercial domains where the interest in high and where risks are more clearly seen, there has been a greater response to the threat of external intrusions. Certainly, the demand for the services of those who make a business of helping companies defend themselves is increasing at a very rapid rate.[31] Threat assessments, sometimes referred to as security risk assessments, commonly identify, qualify, and quantify dangers to our information environment. Although there is an art to threat assessments, most organizations can get either internal or external entities to accomplish the basic technical identification, qualification, and quantification effort. Case in point, Zalmay Khalilzad in Chapter Fourteen of RAND's 1999 Project Air Force Book, "Strategic Appraisal: The Changing Role of Information in Warfare", Defense in a Wired World: Protection, deterrence, and prevention, provides an excellent foundation on information sharing/interconnectivity threats in general. (Page 406). What is often overlooked is the subsequent 'internalization' of the assessment to account for the specific objectives, culture, and stakes of the business. Something that threatens the very existence of one business may not even be applicable to another.

Couched in terms of business value, vulnerabilities reflect the potential costs of inaction in addressing a threat or series of threats. Vulnerability can be direct such as the loss of sensitive data, or indirect, such as the loss of customer confidence or degradation of business reputation. Based upon the threat assessment, a vulnerability assessment depicts the likelihood and impact of the materialization of a threat. The urgency of vulnerability portrays the likelihood, timing and business value of vulnerability. A near-term threat with a high probability of occurrence and large business value would be of high urgency. For a more detailed discussion of terms, see the Talking Eye-to-Eye appendix of this paper.

Synopsizing the threat environment in a chart such as Table 13 provides decision-makers with a quick reference to the topic. Table 13 would allow for threats and recommendations to be presented based upon urgency, business impact potential, vulnerability rating, by mitigation approach, or by what objective (business or IS&S) is impacted. In addition to the columns shown below, and additional columns outlining the objective impacts, performance, costs, and cultural

[29] Andrew W Marshall, "Strategic Appraisal: The Changing Role of Information in Warfare", *Forward*, RAND, Project Air Force, @1999, RAND, page 4

[30] Clayton M Christensen, The Innovator's Delimma, June 1997, Harvard Press

[31] Andrew W Marshall, "Strategic Appraisal: The Changing Role of Information in Warfare", *Forward*, RAND, Project Air Force, @1999, RAND, page 4

impacts of various mitigation mechanisms may also be helpful during the mitigation approach development phase. Finally, charts depicting information product vulnerabilities, mitigation mechanisms and their performance may be useful to develop.

Table 13 - Generic Web Site Threat Chart

Threat/Source	Urgency (likelihood)	Impact Potential (Business terms)	Business Impact Rating	Mitigation Approach(es)
Product information Corruption by hacker or competitor	Possible today but not likely in the near-term	Business Impact –Minor Loss of e-commerce product sales from time of corruption until corruption corrected – Loss of customer confidence in web site	Low	Ensure security features properly configured on web server
Customer information Corruption by hacker or competitor	Six months	Business Impact – Major Loss of orders or orders sent or billed to wrong accounts – Likely to involve limited number of transactions from time of corruption until corruption remedied	Medium	Ensure security features properly configured on web server
Product information theft by insider	Possible today but not likely in the near-term	Business Impact – Nuisance Indicates possible insider vulnerability that should be dealt with. Can be achieved by copying site or company magazine	Low	None
Product information theft by competitor or hacker	Possible today but not likely in the near-term	Business Impact – Nuisance Could indicate vulnerability for more aggressive actions. Can be achieved by copying site or company magazine	Low	Ensure security features properly configured on web server
Customer information theft by insider	Possible today but not likely in the near-term	Business Impact – Catastrophic Loss of customer sales, customer confidence, business reputation Indicates extreme vulnerability within organization	Highest	- Deter by ensuring employees understand consequences of stealing company data - Security Awareness program including safeguarding passwords - Background checks for ADP support personnel
Customer information theft by hacker	Possible today but not likely in the near-term	Business Impact – Catastrophic Loss of customer sales, customer confidence, business reputation	High	- Procure and install security software for customer information database and transactions
Customer information theft by competitor	Possible today but not likely in the near-term	Business Impact – Catastrophic Loss of customer sales, customer confidence, business reputation	Highest	- Procure and install security software for customer information database and transactions - Deter by ensuring employees understand consequences of selling company data - Security Awareness program including safeguarding passwords - Background checks for ADP support personnel
Denial of Service (DOS)	Near term for e-commerce and other internet dependent business	Business Impact – Major Loss of e-commerce business until DOS attack subsides. Loss of internet connectivity with strategic partners until DOS subsides	Medium	- Procure and install DOS prevention software and hardware. - Participate in anti-DOS partnership with neighboring internet sites and routers
Physical Attack	No Foreseeable Actors	Long Term loss of operations	Low	No additional actions required

In general, the generic threats outlined above hold for both the PDD and GCCS scenarios. For the PDD scenario, the PCCIP and PDD 63 reports highlighted the vulnerabilities of insider vulnerabilities, for example system administrators or users divulging passwords and information, and denial of service as the most serious risks. Chapter Nine of RAND's 1999 Project Air Force Book, "Strategic Appraisal: The Changing Role of Information in Warfare", U.S. Strategic Vulnerabilities: Threats against Society, does a good job out outlining and analyzing the threats to the PDD-63 critical infrastructure. Peter Daly emphasizes the importance of business culture and business value to mitigation approaches for NII threats when he states, "In the new national security environment, where private assets may become targets, conventional business models may be inadequate to fully consider the tension between risk and uncertainty. Too heavy a reliance on statistical probability and other quantitative decision theories to guide choices affecting such issues as network security likely will end up causing regret when an exposure assessed financially insignificant in term of probability is exploited by an adversary, causing embarrassment and public alarm that could translate into lost confidence in the enterprise. As a business separates more from the central government, it might do well to adopt some of the politician's high sensitivity to the penalties that are meted out by the public for such "market failures".[32]"

For additional insights specific to the GCCS scenario, chapter ten of RAND's 1999 Project Air Force Book, "Strategic Appraisal: The Changing Role of Information in Warfare", *Implications of Information Vulnerabilities for Military Operations*, (pages 283 – 323) provides a good outline and analysis of the threats and risks to command control, including specific looks at the Global command and control system environment. Although specific to the Air Force, the chapter sorts and analysis the threats into threat categories: Computer Hackers, Traditional weapons, Machinery, Jamming, new weapons, and 'Acts of God, nature, and evil spirits'. (page 288)

Mitigation Approaches:

In many respects, mitigation approaches are where the sharing and security-balancing act begins. Selecting mitigation strategies is a balancing act because:

- sharing normally makes money;
- security usually costs money;
- the more sharable the information, the less secure the environment;
- the more secure the environment, the less sharable the information;
- there is no approach to make an information environment 100% invulnerable; and
- people are the biggest security asset and the biggest security threat.

The balancing act for mitigation approaches can be further complicated by the fact that rarely is there a single mitigation approach for a vulnerability, and rarely is a particular mitigation mechanism unaffected by the other mitigation mechanisms. Mitigation mechanisms vary greatly in effectiveness, cost, and their intrusiveness on sharing. In addition, there is usually a significant dependence between the best mitigation mechanism and the business culture. Assessing the impact of the specific approaches on the overall business culture, as well as on other mitigation approaches, takes on an important role.

If a basic mitigation strategy is not already in place, organizations may find it beneficial to determine an overall mitigation strategy prior to taking on the specific threats. In determining mitigation strategies, it is important to once again return to the business culture. There are two predominant strategies, "detect-protect-respond" of the Government's defense-in-depth model for INFOSEC, and the "resist-recognize-recover" model described by the Computer Emergency Response Team at Carnegie-Mellon[33]. It is important for the organization to determine their

[32] Peter H Daly, "Soldiers, Constables, Bankers and Merchants Managing National security risks in the Cyber Era", Draft, 22 Nov 1999, PIRP, page 16-17

[33] Report by the Joint Security Commission II, DRAFT, DoD and DCI, August 1999, page 20.

overall mitigation strategy to ensure specific mitigation approaches meld with and adhere to the overall strategy.

For whichever strategy is chosen, Zalmay Khalilzad in Chapter Fourteen of RAND's 1999 Project Air Force Book, "Strategic Appraisal: The Changing Role of Information in Warfare", *Defense in a Wired World: Protection, Deterrence, and Prevention,* outlines and details three basic approaches to mitigating information sharing security vulnerabilities: protection, deterrence, and prevention. page 412-432

- *Protection.* Steps taking to directly defend against a threat before or once it begins to materialize.
- *Deterrence.* Actions taken to compel the source of threat not to act. Convincing the threat source that the costs or consequences of carrying out the threat are too high traditionally does this.
- *Prevention.* Actions taken to neutralize a threat at its source before it can materialize or to prevent the source from achieving the capability to carrying out a threat (e.g., denying them technology).

Tools, such as Dr Dobb's *Attack Tree*[34] methodology, exit to assist in developing and weighing at the technical level the options for mitigating threats. Tools such as this play an important role in capturing threats and identifying options, but tend to weigh options based upon technical merits, such as cost and technical feasibility. Although a beneficial and even necessary step to narrow the broad range of options available, these tools often overlook the importance of recurring and non-recurring costs, return on investment information, critical resource requirements, business risk assessment, and clear linkage to business objectives. Organizations often find themselves focused on the specific mitigation to a specific threat instead of focused on what is best for the business overall. Often, it is not security per se that impedes the business's effectiveness or efficiency, rather, it is the specific implementation of a mitigation strategy chosen without proper consideration for culture, business objectives, all the stake holders, and future trends.

Another important aspect often missed during the technical analysis is developing detailed success criteria at both the technical and business levels, linked to the information sharing and security objectives' success criteria, along with monitoring and assessment game plan. Tools and methods for incorporating these aspects in to the security and sharing approach are addressed in chapter 5 of this paper.

[34] "Attack Trees", *Dr Dobbs Journal,* December 1999, acquired through http://www.ddj.com/articles/1999/9912/9912a/9912a.htm on 2/17/2000

3. Addressing technology and the dynamic nature of information uses, information value, information quality and the business environment

Developing an architecture, implementation and subsequent realization that can keep pace with the changing information technology, changing business practices, and, most importantly, the changing threats is key to proposing a realistic information sharing and security approach. By examining trends, both actual and potential, we are more likely to get an information sharing and security approach that is flexible and adaptable in meeting the business's future needs. As illustrated in Table 14 below, this examination can be done based upon four key areas: purpose or use of the information, value of the information, information quality requirements, and environmental considerations.

- Purpose: Information is collected, processed, and disseminated for intended uses, those intended uses are the information's purpose. Although additional uses for the information may be found, and subsequently become purposes, the intended uses play a large role in determining what bundling of process, substance, and format will be employed. Any information for which the purpose includes sharing of the information amongst individuals, enterprise divisions, or between enterprises needs to have the security of that information considered in its bundling.
- Value: The value of information is based upon the actual or potential benefits the enterprise receives from its use. The value of the information also plays a factor in the bundling because organizations will rarely pay for more for an information product than the value of its information. Additionally, the more substantial the information's value and the more that value is decreased by compromise, the more interest the enterprise has ensuring security is addressed in its bundling.
- Quality Requirements: Information quality is an assessment of the information based on eight factors: accuracy, relevance, timeliness, usability, believability, completeness, brevity, and security[35] If the bundling does not maintain or enhance the quality of the information, it will decrease the information's value or may not be suitable for the purpose. and
- Environmental Considerations: Aside from purpose, value, and quality, there are several other factors that drive bundling choices: technology availability, resource availability, threats, Statutory and Regulatory requirements, Consumer confidence, information availability, consumer characteristics and capabilities, provider characteristics and capabilities.

In order to achieve the flexibility and adaptability needed for a workable approach, outlining the key trends in the areas of information purpose, value, quality and environment is required. Will the purpose for which the information is used change? Will changes in the business practices or the business environment change the balance of information value? Are there things that will need to change in the information sharing or security realm in order to support planned business evolution? Will quality factors of the information need to change for the information to retain or increase its value? What other key changes in technology, threats, customer base, or competition capabilities may affect your sharing or security approach?

[35] JP 6-0, Doctrine for Command, Control, Communications, and Computer (C4) Systems support to Joint Operations outlines seven factors. I added the eighth, believability. There must be a level of confidence in the data, whether that stems from a credible source or just that it seems logical.

Table 14 - Common Trends Affecting the Scenarios

Trend Area	Trend	Business Impact	Impact on Sharing	Impact on Security
Information Intended Use	More dynamic information environment with increased emphasis on interactivity and collaboration	More rapid collection, analysis, and dissemination, possibly by moving analysis into either sensor or final exploitation phase	Business Critical	
	Information Warfare	- Increased infrastructure posture (system statuses) information requirements - Increased information requirements on information infrastructure and supporting personnel		Business Critical
Information Value/ Quality	- Increased value/quality on information - Information becomes more perishable - More time constrained to be usable	- Increased vulnerability and urgency as business value of information rises - Increased speed and throughput requirements	Business Critical	Business Crucial
Environment	Dramatic increase in volume of information	Increased dependence on communications, interoperability, and connectivity	Business Critical	
Threats	1) 'Nuisance' hacker vulnerability will decline with fielding of secure computing technology. 2) Increased threats in the Asymmetric warfare category	"Increased threats, both in type and source: Second, the information 'dimension' increasingly becomes central to the outcome of battles and campaigns. Therefore, protecting the effective and continuous operation of one's own information system and being able to degrade, destroy, or disrupt the functioning of the opponent's information system will become a major focus...[36]"		Business Critical
Technology	Maturing and adoption of Secure Computing technology including Multi-Level Security (MLS) network technology			Business Critical
Market Place				
Infrastructure	1) Bandwidth constraint will continue 2) Faster, smaller computational hardware 3) Improved User interfaces allowing less cumbersome devices, move to more 'roaming' technology 3) Costs for hardware software refresh will remain fairly constant	- Information consumers and providers will become more mobile, restrained mostly by the availability of bandwidth - "When considering strategies for managing risk in the cyber era, we cannot become wrapped in the belief that the past or even present are reliable bases for predicting the future…Some fundamental rules of life are being rewritten, from genetics to astrophysics, and new uncertainties abound. In such an era, where change is the norm rather than the a deviation from the norm and economic connection rather than political division is rising as the world's primary organizing principle, some of the largely quantitative means of calculating risk used for national security strategy during the more bordered and static era of the cold war – territory, troop size, missile counts, delivery systems, and throw weights – do not fit well in the new risk environment that is taking shape.37"		Business Critical
Consumer Capabilities and characteristics	1) More computer literate 2) Financially constrained 3) Larger volumes of information available 4) More interactive environment	1) Increasing connectivity and computer literacy of consumers 2) Increased interconnectivity with Strategic and 'ad hoc' partners	Business Critical	
Providers Capabilities and characteristics	1) Financially Constrained 2) Higher volumes of information production 3) Move to web services type information providing interface	Emphasis on getting the right information to the right place at the right time. Countering the myth that everyone needs access to all information, in fact, that such a paradigm may be detrimental to military operations. In the words of Dr Hans Mark, not only doesn't the Sergeant need to know what the General knows; there are cases when the Sergeant should not know what the General knows. Information Overload must also be addressed.	Business Critical	

[36] Andrew W Marshall, "Strategic Appraisal: The Changing Role of Information in Warfare", _Forward_, RAND, Project Air Force, @1999, RAND, page 4-5

[37] Peter H Daly, "Soldiers, Constables, Bankers and Merchants Managing National security risks in the Cyber Era", Draft, 22 Nov 1999, PIRP, page 13

Table 15 - Trends Specifically Affecting PDD Scenario

Trend Area	Trend	Business Impact	Impact on Sharing	Impact on Security
Environment				
Threats	"Today, the creation of most high technology is no longer driven by the traditional national security requirements. Instead, it is commercially oriented, and, while the post cold war world has become in many respects an even more sectarian and violent place, the growing displacement of ideology with commerce as the primary global organizing principle presents a new set of conditions for U.S. national security planners in a high tech world.[38]"	- "Economic, rather than military, crises now pose the most significant threat to U.S. security. The tighter the coupling of the world's financial markets through global information infrastructure, the increasing U.S. reliance on open global markets for prosperity, and the critical U.S. role in anchoring the global economy as a whole, have made economic contagion both a reality and a risk, while military crises have tended to become more confinable in the absence of opposing bloc alliances. - While government have an important role, the development and protection of commercial technology is primarily a business problem, more amenable to business solutions than public policies. This suggests a new set of tolerances for security as well as privacy, and a new style of command an control system that is not exclusively under military or national security apparatus jurisdiction.[39]"		Business Critical
Technology	This new environment will essentially, require an extension of risk calculation from self-interest to the interests of the global financial system as a whole[40].		Business Critical	
Market Place				
Infrastructure	Changing Role of Government in Information Security	"The role of government in general, and the traditional national security establishment in particular, in managing the emergent risks is nowhere near as clearly and widely supported as was government supremacy in national security matters during the cold war. When primary targets were military command and control centers, missile silos, ships at sea, and the like, there was no real question as to who was in charge, and what kind of response alternatives were available in the event of an attack. But today the targets are just as likely to be privately owned assets and commercial information networks as they are defense systems. Moreover, just a financial markets now exert greater influence on governance by insisting on transparency and sound fiscal policies, for example, so does this new risk field exert constraint on traditional law enforcement, intelligence, and military approaches to national security.[41]"		Business Critical
• •	. . .	. . .	. . .	

[38] Peter H Daly, "Soldiers, Constables, Bankers and Merchants Managing National security risks in the Cyber Era", Draft, 22 Nov 1999, PIRP, page 4

[39] Peter H Daly, "Soldiers, Constables, Bankers and Merchants Managing National security risks in the Cyber Era", Draft, 22 Nov 1999, PIRP, page 4

[40] Peter H Daly, "Soldiers, Constables, Bankers and Merchants Managing National security risks in the Cyber Era", Draft, 22 Nov 1999, PIRP, page 26

[41] Peter H Daly, "Soldiers, Constables, Bankers and Merchants Managing National security risks in the Cyber Era", Draft, 22 Nov 1999, PIRP, page 12

Table 16 – GCCS Scenario Specific - Trends Impact on Business

Trend Area	Trend	Business Impact	Impact on Sharing	Impact on Security
Information Intended Use	Sensor to shooter Move to 'sensor to shooter'. For example, some believe long-range precision strike weapons coupled to systems of sensors and to command and control systems will fairly soon come to dominate warfare[42]	More rapid collection, analysis, and dissemination, possibly by moving analysis into either sensor or final exploitation phase	Business Critical	
	Move to 'crises planning' process for all planning	More dynamic information environment with increased emphasis on interactivity and collaboration	Business Critical	
Environment	Dramatic increase in volume of information	Increased dependence on communications, interoperability, and connectivity	Business Critical	
Threats	1) 'Nuisance' hacker vulnerability will decline with fielding of secure computing technology. 2) Increased threats in the Asymmetric warfare category	Increased threats, both in type and source: Second, the information 'dimension' increasingly becomes central to the outcome of battles and campaigns. Therefore, protecting the effective and continuous operation of one's own information system and being able to degrade, destroy, or disrupt the functioning of the opponent's information system will become a major focus of the operational art.[43]" "One of the hottest military publications in China is a book written by two professional soldiers, Colonels in the People's Liberation Army, Qiao Liang and Wang Xiangsui. In it, the Colonels put forth a proposal for a new military strategy of imbalanced power. They advocate moving away from conventional martial doctrine to the concept of "unrestricted war," or multi-tasking of aggression/defense to include acts of direct terrorism, cyber attacks on critical infrastructures, financial attacks on currencies, political interference, and other methods carried out by the military as well as non-military organizations. (Reference from "*China ponders New Rules of "Unrestricted War"*, John Pomfret, Washington Post Foreign Service, The Washington Post, August 8, 1999).[44]"		Business Critical
Technology	Changing characteristics of warfare: [In 2020,] The critical operational tasks will be destroying or disabling elements of an opponent's forces and supporting systems at a distance. Defeat will occur due to disintegration of command and control capacities, rather than due to attrition or annihilation.[45]	Chapter Eleven of RAND's 1999 Project Air Force Book, "Strategic Appraisal: The Changing Role of Information in Warfare", Military Organization in the Information Age: Lessons from the World of Business, outlines the effects of 'flatting', 'formatting' and concentrating on core competencies, all of which are direction within DOD. All these moves add dependence on the information infrastructure, add risk to the information flow disruption, and increase the importance of information sharing security as the need for information sharing increases. In the latter part of the chapter, the need to address training and personnel is addressed.(Page 327-360)	Business Critical	
Market Place				
Providers Capabilities and characteristics	1) Financially Constrained 2) Higher volumes of information production 3) Move to web services type information providing interface		Business Critical	
. .	. . .	. . .	. . .	

[42] Andrew W Marshall, "Strategic Appraisal: The Changing Role of Information in Warfare", Forward, RAND, Project Air Force, @1999, RAND, page 4-5

[43] Andrew W Marshall, "Strategic Appraisal: The Changing Role of Information in Warfare", Forward, RAND, Project Air Force, @1999, RAND, page 4-5

[44] Peter H Daly, "Soldiers, Constables, Bankers and Merchants Managing National security risks in the Cyber Era", Draft, 22 Nov 1999, PIRP, page 21

[45] Andrew W Marshall, "Strategic Appraisal: The Changing Role of Information in Warfare", Forward, RAND, Project Air Force, @1999, RAND, page 4-5

4. Pulling it all together

With the previously developed charts as supporting documentation, presenting the decision maker with a once over view of the objectives, issues, concerns, players, and business value making up the approach can be invaluable to obtaining the support and direction needed. While organizational dynamics and priorities may dictate its layout and content, a final chart can be developed that succinctly represents the proposed information sharing and security answers, with sufficient justification and background for decision-makers to reach a sound conclusion. Below is a sample summary chart, the content and make-up may vary based upon the business dynamics and the question or tasking originally given. The essence of this chart should be to succinctly represent the proposed information sharing and security answer and sufficient justification and background for decision-makers to reach a sound conclusion.

Table 17 - Sample Prioritized IS&S Recommendations

Objectives	Recommendation	Priority	Business value and Costs	Key Stakes and Stake holders	Issues/ Dependencies	Risks and Trade-offs

Aside from the format of the chart, how is the content of the chart determined? A prioritized presentation of the options would be valuable, but how are options to be racked and stacked, prioritized, and weighed against the other factors and concerns that have been discussed? Chapter 5, on business processes, discusses managing the IS&S approach within the overall business model, but how is the IS&S approach itself determined? There is no single answer to this question. Prioritizing resources and trading off options tends to be organization unique processes, highly dependent on organizational dynamics, culture, and politics. However, here are some general considerations.

The information can be related to and then arrange by objective. This would facilitate and focus discussion on sets of recommendations (sharing mechanisms and mitigation approaches) that satisfy the objective. Accounting for business value, culture, stake holders, trends, and feasibility, these sets of actions can then be analyzed to develop the best set of recommendations for each objective. Developing multiple sets of recommendations can help to identify options and clarify recommendations.

For example, suppose an organization developed four sets of recommendations for each objective: 1) the 'bare minimum' or '80% solution' emphasizing costs and time, often developed to 80% budget or functionality; 2) the 'Sharing Utopia' gives priority to sharing over security, waiving cost and time constraints; 3) the 'Security Utopia' gives priority to security over functionality, waiving cost and time constraints; and 4) the 'Compromise' which reflects the optimal functionality and security mix that falls within reasonable cost and timing constraints. The different emphases of the first three sets enable the development of the fourth set by highlighting community minimums and showing the realm of the possible. In addition, if the various sets of recommendations are developed and debated by the various stake holders, there is opportunity for expanded understanding and buy-in for the overall approach by the stake holders.

As these sets of recommendations are developed, identifying dependencies between recommendations, either for technical or cultural reasons, may be beneficial when funding and budgeting discussions are undertaken. Also, identifying conflicting (if this recommendation is done, the other recommendation cannot be done) or overlapping (if this recommendation is done, the other recommendation need not be done) recommendations will also be beneficial. Once the sets of recommendations are established, they can be prioritized.

Consider categorizing instead of straight numerical ranking for prioritizing recommendations. In addition to often saving time because recommendation proponents are not debating over one or two numerical rankings, categorization lessens the chance of sending an incorrect signal when two recommendations are of equal importance. Take, for example, categories such as 'must do', 'highly recommended', and 'optional'. Such categorizations often serve to more easily separate the recommendations into the top categories while also highlighting to management and stake holders the likelihood of a recommendation being acted upon. 'Must do', the highest priority, would be recommendations guaranteed funding because they have a reasonable risk of success and: a) address a near term business critical security threat; or b) enable sharing mandated by senior management or business forces. Highly Recommended would be recommendations that: a) are deemed to play a significant role in accomplishing an objective as reflected in the recommendation's business value; b) address a medium to long term[46] business critical threat; or c) mitigate a near term business crucial threat. The optional category are recommendations that, time and money permitting, will be addressed - reflecting the realism that in many business venues there are recommendations that do not represent a significant enough business value or address a significant enough threat to be funded.

If the IS&S project funding line falls within a category, or a finer ranking of recommendations are needed for resource management, rank ordering of the potentially funded recommendations may be required. However, the initial categorization may enable entire categories of recommendations to be dismissed from the ranking process if the category falls completely inside or outside the funding lines.

Once the prioritization is complete, financial and other constraints can be applied to produce the recommended IS&S approach. There is significant benefit to getting key stakeholder buy-in on this recommended approach before submitting the proposal to upper management for approval.

[46] Setting medium term as two project funding cycles and long term as three or more funding cycles allows these recommendations to move up in priority if not addressed in the current cycle.

Table 18 – Prioritized GCCS Information Sharing & Security Recommendations

Objectives	Recommendation / Priority	Benefits and Costs	Key Stakes and Stake holders	Issues/Dependencies	Risks and Trade-offs
Single Workstation Access for GCCS	Automatic Security Data labeling of electronic data / Must Do	Enables MNS[47] and MLS solution. Costs would vary greatly depending on data labeling scheme. Allowing the DBMS to automatically set the security level based upon the Network from which the data is received, with limited downgrade by authorized personnel, would be a cost effective approach. Costs (Est)- $500K	DISA and war fighters assigned responsibility for downgrading information	Prerequisite for MNS and MLS recommendations	Feasible today
	Multiple Secure networks (MNS) (See 'Talking Eye-to-eye Appendix) /Must Do	1) Business value added assessment: a) Significant Operational Efficiency increases b) Decreased information dissemination time as manual steps are removed c) Fewer ownership confusion problems as the need to copy data to multiple networks is reduced d) Less vulnerability as a result of less confusion over the real classification of information. e) More secure – Non-perfect trusted products are less vulnerable than perfect untrusted software f) Trusted computing products are a need for both the private and public sectors. However, these products can become technically or financial viable to the product producers and consumers if they are not brought in operation and matured. It is better to do this now than after the ideas of information warfare are more widely accepted and the threats during the maturation process are too high. 2) Business costs a) Implementation costs for JOPES databases only (assuming five data servers and no client software changes required) merging GCCS and GCCS-T database and creating NIPRNET accessibility – (est) $1 Million b) Operational and Technical support training – (est) $500K	See attached Stake holders chart	1) Highlights of the implementation: a) Procedural solutions may be needed to address some shortfalls of the maturity of the trusted software solutions (e.g., limiting the folks that can do downgrades, marking print outs) b) Each LAN is assumed to be accredited and trusted to the security level it is approved for (i.e., the US accepts all those connected to the ALLIED LAN as suitable for processing SECRET information). c) There are multiple technically feasible and economically viable realizations of the MNS from the ADP perspective; i) one MLS server containing all information (of a particular type) with duplicated systems for performance and back-up ii) an MLS server for each level of data using distributed database technology to make it appear to users as one database; or iii) set of geographically determined MLS data server 'populated by proximity' using modern data synchronization to maintain data integrity and reliability are few such possible instantiations of the concept. iv) Various methods for attaching or implying data classification label d) Security Awareness and technology training will be key to a viable realization development.	The availability of secure operating systems[48], secure database tools[49], and other trusted software packages[50] make this a viable solution
	Multiple Level Security (MLS) Network /Future Must Do	Recommended as long term, evolutionary effort dependent on implementation of MNS recommendation		MLS server, such as those implemented in the MNS recommendation must be implemented	Technology not yet available. Can be built on top of MNS solution.

The tools and ideas presented in the preceding section may not reduce the overall time and effort involved in developing a viable information and sharing approach, but they will help to organize, address, and present the effort for presentation to senior management.

[47] For discussion on MNS and MLS technology, see the 'Talking Eye-to-eye' Appendix

[48] Sun Microsystems (www.sun.com) has a secure operating system which they feel is accreditable to the B1 level of trust

[49] Sybase (www.sybase.com) and Oracle (www.oracle.com) have secure DBMS products that when implemented on a B1 OS, provide B1 level of trust for database functions

[50] Trusted Computing Solutions (www.tcs-sec.com)

Chapter 5: Business Processes – The Balancing Act

Sharing and security represent both recurring and non-recurring costs in technology, administrative, people and infrastructure. Information sharing and security requirements must be assessed, prioritized, and traded off with other business requirements. What is needed is an approach to the management of information sharing and security that is both inclusive – whose scope truly reflects the potential contribution of information – and more specific. To be meaningful to business managers, the management console for information sharing and security must go beyond attractive concepts to specific measures that are business related. To do this, information security and sharing must be put into business value terms and directly incorporated into the overall enterprise management processes.

However, adapting Peter Daly's and Charles Popper's information technology concepts, we can deduce that despite efforts to develop guiding principles for management of the information sharing and security function, the core dysfunction remains: most businesses have not yet attained the level of business/Information Technology alignment and integration desired by senior management. Business leaders often lack a clear understanding of how information sharing and security can contribute to their business success; even more often, they cannot reconcile the growing costs of information technology with their perception of the value received.[51]

At the same time, security advisors and information technology advocates must realize that the enterprise does not have infinite resources, therefore it may be beneficial to present options of varying cost and effectiveness. By avoiding all or nothing approaches and ensuring the decision-makers are fully informed on the vulnerabilities and urgency associated with each proposal, senior management will be able to better balance IS&S requirements within the larger business context.

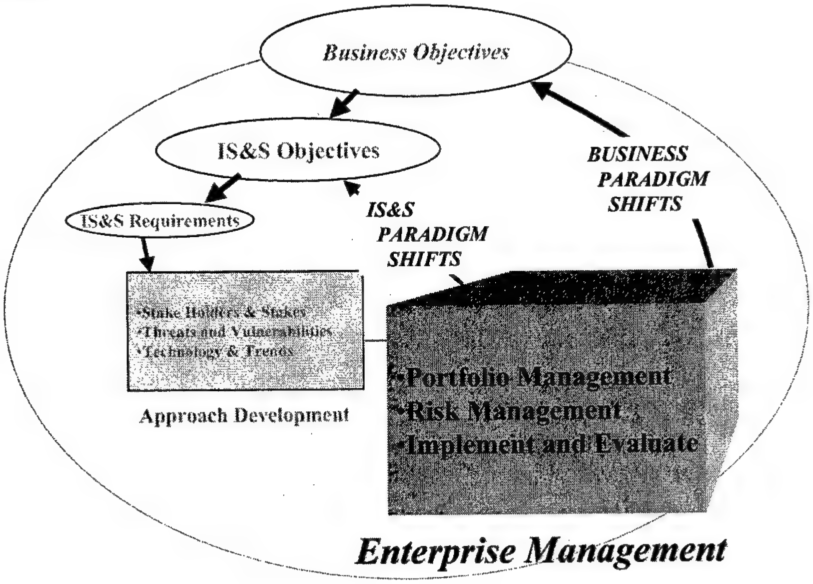


Figure 6 - IS&S: Bringing the Approach in To the Organization

[51] Peter H. Daly, *Soldiers, Constables, Bankers, and Merchants: Managing National Security Risks in the Cyber Era,* DRAFT, November 1999, Harvard's Program on Information Resources Policy, page

Instituting well defined evaluation programs, managing security and sharing efforts as portfolios, and incorporating IS&S into the overall business risk management scheme may be the key to successful IS&S balancing. Both Peter Daly and Charles Popper discuss these topics in detail. Presented below is a brief discussion of the topics.

1. Portfolio Management

Information sharing and security efforts are laced with interdependencies. Often, the success of one mitigation approach is directly dependent on the success of another mitigation approach. Changes in one mitigation approach's schedule, technology, or functionality can drive changes to other mitigation approaches. Portfolio management of information sharing and security could alleviate problems resulting from such implementation dynamics. In addition, if the ability for the organization to share certain information or accept certain information partners is dependent on an underlying security mechanism, portfolio management of these efforts may also be beneficial. As discussed earlier, information sharing and security implementations often impact the business culture, which then require efforts to address awareness, training, technology, policies and procedures.

The operational community cannot properly do sharing and security without the security community, and neither community can properly do it without the support (system developers/maintainers) community. Security implementations drive not only operational constraints, but also costs in support (ADP, Training, and developers) people, security people, acquisition, and system resources (Bandwidth, computing power, data duplication, procedures, processes). Furthermore, a security strategy must address communications security, computer security, and operational security.

The existing GCC/GCS management structure provides an acceptable forum for information sharing and security approach development and implementation. The GCC/GCS Advisory Board is comprised on senior level stakeholder representatives and is chaired by the war fighting communities, the major stakeholder for command and control. However, that charter of the GCC Advisory Board, GCC Review Board, and GCC requirements Board must be modified to move information security requirements from technical requirements, prioritized and funded separately from business's functional requirements, to the functional requirements category.

2. Risk Management

"The advent of the information age will require, as never before, that we take a wider perspective and avoid stovepipes that blind us to changes taking place outside our own sphere of direct responsibility.[52]"

What should be traded-off, information sharing efficiency, information sharing effectiveness, customer trust, security risks, or partnership relations? Pulling together the results of the trend analysis, current approach assessment, and the identification of areas of improvement, develop proposed changes to the enterprise's information sharing and security approach. Programmatic changes, often the most economical, reflect ways of doing the current process better, perhaps automating some tasks. Evolutionary changes reflect a natural progression of the approach to account for changing technology or environment. Revolutionary changes, often the most risky, reflect fundamental ways of changing the manner in which the

[52] Andrew W Marshall, "Strategic Appraisal: The Changing Role of Information in Warfare", Forward, RAND, Project Air Force, @1999, RAND, page 2

enterprise does information sharing and security. Charles Popper provides additional insight and mechanisms for evaluating and portraying such changes in his paper entitled "A holistic framework for IT governance."[53]

Information sharing and security has the potential to change or prohibit the changing of basic business functions. Often referred to as a disruptive technology[54][55], the potential impact of information sharing and security on an organization can be far reaching. Therefore, the appropriate level and amount of involvement of senior business management can determine the success of the business[56]. The goal is both informal dialogue and formal decision making. Ongoing dialogue is needed for the management to fully understand the planned use of technology and its impact upon the business and to elicit their guidance, feedback, and strategic instinct. Formal decision-making helps to ensure that critical decisions are fully committed to by all groups in the enterprise. Finally, senior management can best assess progress toward business value.

Although there are many proven techniques to accomplish this, Charles Popper points out that they all boil down to a few common principles. First, a group of senior managers must accept formal responsibility for strategic decisions regarding information sharing and security. This should be an existing management committee or, if necessary, a dedicated information sharing and security committee. Second there must be agreed processes to identify the decisions to be made, to collect, analyze and disseminate the data needed to make informed decisions, and to make and communicate decisions. These decisions processes should not differ in principle from those used in managing all aspects of the enterprise. Third, the senior managers must be involved on a regular basis, not just after project disaster, but proactively, setting priorities and establishing and revisiting strategies. Today's business world is far too dynamic to implement strategy via remote control. The life cycle of a typical information technology project may often exceed that of the underlying business strategy; hence, management vigilance and participation is essential.[57]

The existing GCC/GCS management structure provides an acceptable forum for information sharing and security approach development and implementation. The GCC/GCS Advisory Board is comprised on senior level stakeholder representatives and is chaired by the war fighting communities, the major stakeholder for command and control. However, that charter of the GCC Advisory Board, GCC Review Board, and GCC requirements Board must be modified to move information security requirements from technical requirements, prioritized and funded separately from business's functional requirements, to the functional requirements category.

3. EVALUATIONS

As discussed, information sharing and security has many facets. As such, the evaluation of the impact of information sharing and security approaches should also be

[53] Charles Popper, "A Holistic Framework for IT Governance", January 2000, Harvard's Program On Information Resources Policy (PIRP), copyright 2000

[54] Clayton M Christensen, The Innovator's Delimma, June 1997, Harvard Press

[55] "Schumpeter, Joseph Alois," Microsoft® Encarta® Online Encyclopedia 2000 http://encarta.msn.com, ©1997-2000 Microsoft Corporation. All rights reserved. © 1993-2000 Microsoft Corporation.

[56] This is seconded by GAO Executive Guide, "Information Security Management: Learning from Leading Organizations," May 1998, GAO/AIMD-98-68 Information Security Management, which highlights the point that "Senior Executive Support is Critical" in discussions on information security.

[57] Charles Popper, "A Holistic Framework for IT Governance", January 2000, Harvard's Program On Information Resources Policy (PIRP), copyright 2000, page 11

many faceted. First, there is the technical feasibility and assessment: 'is it doing what it was designed to do?" Next, is the business value assessment: 'do the benefits justify the costs?" Third is the business culture impact: have changes in the information sharing and security approach changed the business culture (how we do business) or do changes in business culture require changes to the information sharing and security approach?

The technical and return on investment evaluations are fairly common and well documented activities for individual development and implementation efforts. However, assessing the overall business value across the whole information sharing and security approach is not as common, and not as straightforward. Accomplishing an assessment on the impact of the information and sharing approach on the business culture is an even rarer activity. However, it is the latter two activities that can portray the true impact of the approach on business and also be the most understandable by senior management.

Returning to anti-virus software as an example: evaluations on the number and types of viruses that have been encountered on the business's information infrastructure; details of the software's performance; and cost data including the procurement, implementation, maintenance, and operation of the software could all be collected and analyzed against actual or projected loss of productivity, clients, or other business factors. The business value success criteria discussed earlier calls for the assessment of the composite of approaches, also called a portfolio, correlated to each objective, allowing for the analysis of progress towards the overall business objectives and enterprise-wide business value. Such assessments may lead to discoveries like the implementation of anti-virus software allows the business to relax the ban on employees bringing diskettes in from home. Or that the anti-virus software has been ineffective because of a failure in the associated security awareness effort.

With the speed at which business practices are evolving, identifying and capitalizing on new business techniques can be a key facet in the new risk-based business model. Taking the assessment to next step of examining business culture impacts has a two-fold effect: looking for expected revolutionary impacts, and finding unexpected revolutionary impacts.

Appendix A: *Talking 'Eye-to-eye' - A Language Framework.*

Being able to communicate clearly and concisely about a topic is dependent not only on the linguistic dexterity and competence of the presenter, but also on those of the audience. Effective communication is critical to any effort's success, therefore, before your organization can embark on addressing information sharing and information security, there are a number of words and phrases denoting underlying concepts that the parties involved must have a common understanding of. The following section provides the foundational common framework of understanding, giving organizations the basic tools needed for addressing information sharing and security concepts. However, this language framework is only a starting point. Continued dialogue and vigilance is needed to ensure parties involved communicate effectively.

This paper does not distinguish between data, information and knowledge. One man's knowledge is often another man's information, and may only be a data point to a third. What a front-line worker may "know" is often information or even just data to corporate staff, yet the substance is the same. Philosophers, dating back to Aristotle and Plato, have engaged the definition question, and no lasting consensus has emerged.[58]

What is an Information Sharing and Security Approach?

Using the context presented later in this section, an information sharing and security approach is a set of information sharing and security objectives with a plan for influencing the enterprise's information process, substance, and format bundling to accomplish those objectives.

- *Information sharing and security objective.* A measurable concept on which a business objective or goal is dependent on the concept's full or partial accomplishment. The paper uses the structure that the business goals are the aims of the organization, and that one or more business objectives, if met, will achieve those goals. Goals tend to be more vague, while objectives are specific and quantifiable. Information sharing and security objectives should focus on enabling the business objectives and should be phrased in a positive tone. From the objectives, overall information sharing and security stakes for the enterprise should be evident.
- *Information process, substance, and format bundling* (see below)

[58] William H Read, "Knowledge as a Strategic Business Resource", Incidental Paper, Program on Information Resources Policy, Harvard University, Cambridge, Massachusetts, Copyright 1999 by President and Fellows of Harvard College, page 1.

What is Information?

> *"Information is a basic resource, like energy and materials. Without materials there is nothing; without energy nothing works; and without information, nothing makes sense.*[59] *"*
>
> - Dr Tony Oettinger, Program on Information Resources Policy

In discussing information, being able to articulate which aspect in particular of information products is of concern enables us to more clearly paint the desired picture. Below is an adaptation of Harvard's Program on Information Resources Policy (PIRP) portrayal of information product elements. Additional detail and illustration of the PIRP's portrayal can be found in Martin Ernst's book, "Mastering the Changing Information World."

"Media may come and media may go, but the basic substance, format and process building blocks stay on as the tools of choice for expressing change. Thinking explicitly in terms of these building blocks helps avoid entrapment in bundles tied by the exercise of discretion appropriate to the moment in history but whose time may be long gone.[60]

Information products and services are built from a triad of elements:

- *Substance:* Refers to the content of the information in a very broad sense; Data, knowledge, and the rest are kinds of information substance – of greater or lesser value, of greater or lesser cost. Out of the broader notion of information resources, the concept of substance brings out the essence of information, the thing that is either a picture or a thousand words conveys, the thing evoked when speaking of matters that are substantive rather than formal or procedural.[61]
- *Format:* Concerns the physical materials and/or signals in which substance is, or can be, embodied for subsequent manufacturing and distribution as well as for eventual absorption and interpretation; and
- *Process:* Includes all the energy-consuming means used to create and manipulate substance, embody it in a format, and deliver it to a user"[62] Dr Frederick P. Brooks, Jr conceptualizes processes as having three components, the architecture (plan), the implementation (concept for carrying out the plan), and the realization (a specific instantiation of the implementation)[63][64]
    - *Architecture:* The conceptual plan for outlining the strategy to achieving the business objectives[65]: People talk about business architectures,

[59] Ernst, Oettinger, Branscomb, Rubin and Winkler, "c", page 21, Ablex publishing Corporation, Norwood, New Jersey, copyright 1993

[60] Ernst, Oettinger, Branscomb, Rubin and Winkler, "Mastering the Changing Information World", page 49, Ablex publishing Corporation, Norwood, New Jersey, copyright 1993

[61] Ernst, Oettinger, Branscomb, Rubin and Winkler, "Mastering the Changing Information World", page 26, Ablex publishing Corporation, Norwood, New Jersey, copyright 1993

[62] Ernst, Oettinger, Branscomb, Rubin and Winkler, "Mastering the Changing Information World", page 7, Ablex publishing Corporation, Norwood, New Jersey, copyright 1993

63 Blaauw, G.A., and F.P.Brooks, Jr., "Computer Architecture: Concepts and Evolution", Addison-Wesley, copyright 1997, pp 3-31

[64] Bernard Cohen, "Howard Aiken: Portrait of a Computer Pioneer", The MIT Press, Cambridge, Mass., Massachusetts Institute of Technology, copyright 1999, page 144

[65] Anthony Oettinger's presentation to Harvard's GEN ED 156 seminar, October 1999.

  information architectures, security architectures, and even information technology architectures as separate, often overlapping, entities. What we need to do is talk about a secure information technology architecture for our business.
  - *Implementation:* The rules and guidance level of detail outlining the approach to be taken to accomplish the architecture; and
  - *Realization:* The actual application of materials, energy and information representing an instantiation of the implementation.

- *Bundling.* Information products can be described as a combination or *bundling* of process, format, and substance. Often the names of the product distinguish the bundling and provide us insight. For example, Television news versus newspaper. The terms themselves give us an indication that even though the substance may be the same, the process and format are different. However, the biggest advantage to this language framework is the removal of ambiguity when addressing information and information products by providing a set of tools to clearly express ideas, concepts and concerns.

		Bundling 1	**Bundling 2**
Element	**Component**	**'Feline Stories'**	**'Classified Letter'**
Substance		Story about Garfield	SECRET Letter From Joint Staff J6
Format	Symbol	A representation of a feline	A SECRET label on the top of the document
	Pattern	The English word 'CAT'	The word 'SECRET" on the top Center of the page
	Token	A transistor is in 'on' state	A smudge of ink on the paper
Process	Architecture	Collecting and storing stories about famous felines where anyone have access to them free	Classification System which prevents sensitive US Government information from falling into the wrong hands
	Implementation	Copying all the stories we can find in libraries on a web site	Classification levels of TOP SECRET, SECRET, UNCLASSIFIED, with special releasability caveats, handling, protection, and information labeling procedures and processes
	Realization	An SUN SPARC web server at URL www.cats.com containing all the scanned stories on cats from the Watertown Public Library in a Sybase DBMS	A system of labeling, handling, storing, protecting, and discarding US Government paper documents

Table 19 - Elements and Components of an Information Product

Bundling Drivers. Which bundling is chosen, and that bundling evolves or is replaced, for any particular piece or category of information product is based upon four key areas: purpose or use of the information, value of the information, information quality requirements, and environmental considerations.

- *Purpose:* Information is collected, processed, and disseminated for intended uses, those intended uses are the information's *purpose*. Although additional uses for the information may be found, and subsequently become purposes, the intended uses play a large role in determining what bundling of process, substance, and format will be employed. Any information for which the purpose includes sharing of the information amongst individuals, enterprise divisions, or between enterprises needs to have the security of that information considered in it's bundling.
- *Value:* The *value* of information is based upon the actual or potential benefits the enterprise receives from its use. The value of the information also plays a factor in the bundling because organizations will rarely pay for more for an information product than the value of its information. Additionally, the more substantial the information's value, and the more that value is decreased by compromise, the more interest the enterprise has ensuring security is addressed in its bundling.
- *Quality Requirements:* Information quality is an assessment of the information based on eight factors: accuracy, relevance, timeliness, usability, believability, completeness, brevity, and security[66] If the bundling does not maintain or enhance the quality of the information, it will decrease the information's value or may not be suitable for the purpose. and
- *Environmental Considerations:* Aside from purpose, value, and quality, there are several other factors that drive bundling choices: technology availability, resource availability, threats, Statutory and Regulatory requirements, Consumer confidence, information availability, consumer characteristics and capabilities, provider characteristics and capabilities.

What are Stakeholders?

Who has a vested interest in an organization's approach to security? Traditionally, stakeholders have been categorized as consumers and providers of information, and, in some instances, its protectors. With the move into global interconnection and interdependence, the list of traditional stakeholders expands to include global consumers, providers, and protectors of information. The explosion of information usage has precipitated a shortage of information support resources; increasing the importance of the information infrastructure developers/maintainers, information sources and information owners.

[66] JP 6-0, Doctrine for Command, Control, Communications, and Computer (C4) Systems support to Joint Operations outlines seven factors. I added the eighth, believability. There must be a level of confidence in the data, whether that stems from a credible source or just that it seems logical.

- Traditional Stakeholders: It is not uncommon for the business conducting entity to be an information consumer, information provider, and information protector. These are, however, divisible roles.
    - *Consumers.* The entities that use and exploit the information to realize its business value.
    - *Providers.* The entities that collect, analysis, and disseminate information to consumers.
    - *Protectors.* Entities tasked with advising and enforcing information security.
- Expanded Stakeholder list
    - *Global consumers.* Special categories of information consumers, global consumers are those entities outside the enterprise that use the enterprise's information. Because of the business benefits of globalization, this category of consumer must be considered in the information sharing and security approach from the aspects of interoperability and information accessibility.
    - *Global Providers.* Special categories of information providers, global providers are those entities outside the enterprise that supply enterprise information. Because of the business benefits of globalization, this category of provider must be considered in the information sharing and security approach from the aspects of compatibility, interoperability and information availability.
    - *Global Protectors.* Special categories of information protectors, global protectors are those entities outside the enterprise that protect enterprise information between enterprises. This category of protector must be considered in the information sharing and security approach from the aspects of compatibility, interoperability and information vulnerabilities.
    - *Information owner.* The entity with the ultimate jurisdiction over the information. The information owner is the authoritative body for decisions pertaining to information sharing and security requirements. In the new global market, as information is duplicated and distributed worldwide, it is important to identify the information ownership. Failing to meet the information owner's expectation for security may result in the owner rescinding your right to use their information.
    - *Information sources.* The entity, either internal or external, from which the information is obtained.
    - *Information infrastructure developers and maintainers.*
        - *Information technology providers.* Those entities on which the enterprise relies for information technology. Information technology providers include commercial software vendors, hardware vendors, and communications vendors, as well as internal enterprise resources. Understanding these entities business directions, as well as both their capability and desire, in providing information sharing and security technology are a key

considerations in formulating information sharing and security architecture, implementations, and realizations.

- *Enterprise Information Infrastructure Developers.* Those entities responsible for the initial realization and advancement of the enterprise's information infrastructure. Understanding these entities business directions, as well as both their capability and desire, in providing information sharing and security realizations are a key considerations in formulating information sharing and security architecture, implementations, and realizations.

- *Enterprise Information Infrastructure Maintainers.* Those entities responsible for ensuring the proper operation of the underlying information handling and processing tools. Most commonly seen as the automation support organization, this organization must have the capabilities, both in resources and tools, available to accomplish their portion of the information sharing and security approach.

What are Stakes?

Understanding each stakeholder's opportunities and risks is crucial. Just as important is recognizing the potential consequences of each security approach on each stakeholder. Pulling your finger out of the dike and running may only get you wet, but it may ultimately flood the village. Another emerging aspect of the global market coupling is the far-reaching impacts one entity can have on others. Capturing and quantifying each stakeholder's contributions and requirements is key to the framework.

What is Information Sharing?

Information is shared in a variety of ways and for a variety of reasons. The term *information sharing* is used as opposed to *information exchange* because *exchange* implies a two-way flow. It is important to note that information can be shared unintentionally as well as intentionally. Additionally, information sharing refers to information shared electronically, orally, hardcopy, and visually.

What is Information Security?

"*Business is war. Survival of the fittest. In order to survive in today's cutthroat business environment, we must be properly armed. One of the most important arrows in the businessman's quiver is accurate knowledge of his competitors and business environment... Possessing accurate intelligence is like having a flashlight in the dark. It won't remove any obstacles in your path, but it will illuminate them so you don't stumble.*[67]"

Protecting information is rising in importance as quickly as information usage is rising. However, what does information security mean? A multitude of terms used by the various players muddies the water and degrades information security efforts. Within DOD, war fighters employ operational security (OPSEC), NSA and ADP personnel

[67] RW Rustmann Jr., "The Craft of "Business" Intelligence", INTELLIGENCER, Association of Foreign Intelligence Officers, August 1999, Copyright 1999, page 4

discuss ponder computer security (COMPSEC), communications technicians strive to improve communications security (COMSEC), even though the terms have been officially merged into a common term, information security (INFOSEC). At the same time *information assurance* is being touted as the protector of information quality and availability while *information protection* and *defensive information warfare* appear to refer to steps taken to stem the effectiveness and impact of threats.

The variety of terms and definitions stem from the varying vantage points to an information security communications problem, further emphasizing the need to ensure these various entities have a common language framework.

Information security is steps taken to ensure the organization is not prevented from realizing the purpose, value, and quality of their information while ensuring the organization's business advantages are not compromised by external information collection efforts. Information security is discussed in terms of:

- *Threats.* The term threat is used to refer to any potential compromise of information or information quality. Traditionally, a threat has a source and potential consequence. Threat sources can be internal such as an untrained computer operator accidentally deleting the enterprise database, or external, such as industrial espionage efforts. A threat's consequences are described in actual terms, meaning the actual information compromised or quality impact if the threat were to materialize. Zalmay Khalilzad in Chapter Fourteen of RAND's 1999 Project Air Force Book, "Strategic Appraisal: The Changing Role of Information in Warfare", *Defense in a Wired World: Protection, deterrence, and prevention*, provides an excellent foundation on information sharing/interconnectivity threats in general. (page 406)
- *Vulnerability.* A potential loss or negative impact. Vulnerabilities reflect the potential costs of inaction in addressing a threat or series of threats. Vulnerability can be direct such as the loss of sensitive data, or indirect, such as the loss of customer confidence or degradation of business reputation. Vulnerabilities are quantified in terms of business value. The term vulnerabilities is used, as opposed to security risks, because 'risk' has several contexts, including referring to the likelihood of success of a venture. It is would noting that it common in the security community to use term risk and risk assessment in the same vein as vulnerability and vulnerability assessment are used in this paper.
- *Threat assessments.* The likelihood of a threat materializing in the near term, mid-term, or long term.
- *Vulnerability assessment.* Based upon the threat assessment, a *vulnerability assessment* is accounts for both the likelihood and impact of the materialization of a threat. The *urgency* of a vulnerability portrays the likelihood, timing and business value of a vulnerability. A near-term threat with a high probability of occurrence and large business value would be of high urgency.
- *Mitigating Actions.* Actions taking to thwart a threat or to lessen its potential impact. Zalmay Khalilzad in Chapter Fourteen of RAND's 1999 Project Air Force Book, "Strategic Appraisal: The Changing Role of Information in Warfare", *Defense in a Wired World: Protection, deterrence,*

and prevention, outlines and details three basic approaches to mitigating information sharing security vulnerabilities: protection, deterrence, and prevention. page 412-432

- *Protection.* Steps taking to directly defend against a threat before or once it begins to materialize.
- *Deterrence.* Actions taken to compel the source of threat not to act. Convincing the threat source that the costs or consequences of carrying out the threat are too high traditionally does this.
- *Prevention.* Actions taken to neutralize a threat at its source before it can materialize or to prevent the source from achieving the capability to carrying out a threat (e.g., denying them technology).

An *information sharing and security approach* must address the key components of *awareness, training, technology, policies* and *procedures*.

- *Awareness.* Making sure your most important resource, people, understand what information needs to be secured and why. The consequences to the business and the individual must be understood.
- *Training.* A program that teaches peoples how to secure information.
- *Technology.* The use of automation and other tools to secure information.
- *Policies.* Clear, concise statements portraying the business's philosophy and approach to information security.
- *Procedures.* Step by step instructions on how to perform security tasks and actions.

Getting Technical

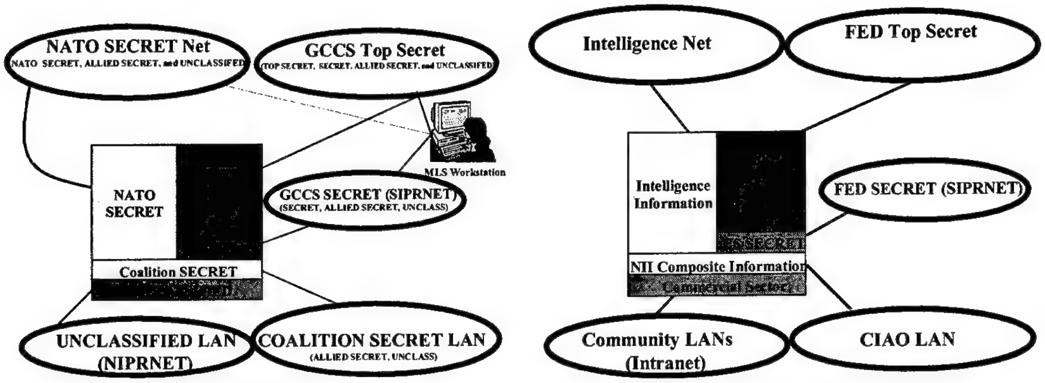
a) ***Confidentiality Levels.*** Categorization of information indicating the desire to limit the access to or exposure of the information. In the Government, the term security classification is used and the labels UNCLASSIFIED, SECRET, and TOP SECRET, along with a book full of caveats, downgrading instructions, and rules indicate some of the confidentiality level of information. In business, terms such a PROPRIETARY, CONFIDENTIAL, and DEPARTMENTAL USE ONLY are used to indicate that special handling of the information is desired.

b) ***Data Labelling.*** Whether accomplished by placing a stamp on the page, placing the report in a special folder, or electronically marking data in a database, *Data labeling* is the term used to refer to placing a confidentiality level marking on data.

c) ***Multiple Network Security.*** In a nutshell, a multiple network security approach having networks at various classification levels, strategically interconnected by secure computing devices. Although each network is at a single classification level, users can access and change data on their LAN and see selected data on lower classification LANs. However, any data that is added or modified must enter the network at the classification level of the higher LAN. A separate step is then required to 'downgrade' information, if appropriate and desired, to the lower classification. Two basic types of technology are available for such an implementation: secure gateways or firewalls; and multiple security level data servers.

i) *Firewalls* function by controlling the flow of information between the two networks. With firewalls, the user (or an automated agent on behalf of the user) travels out onto the other network and retrieves the data.

ii) *Secure data servers*. With secure data servers, the information at the various classification levels resides on the data server. The secure server allows authorized users entering to see data from the lowest classification level up to and including the classification level of the LAN where the user entered the server from ('look down' approach). The user cannot see data of other equal or higher classification levels (no side or up look). Data entered by a user is labeled at the security level of the LAN, and a separate step is required for the user to downgrade the data. (Downgrading data means lowering the classification level, reclassifying data means the user changed the compartment or country releaseability markings of data). There is no requirement for information destined to or from the data server to travel on any LAN outside the users LAN (i.e., all data requests/communications are between the user's workstation and the data server). This does not mean that the a distributed database could not exist at a particular security level, entailing the two data servers to then communicate to access/store distributed data.



Example GCCS MLS Data Server

PDD Support MLS Data Server

Figure 5 - Multi-Network Secure Server: Conceptual Examples

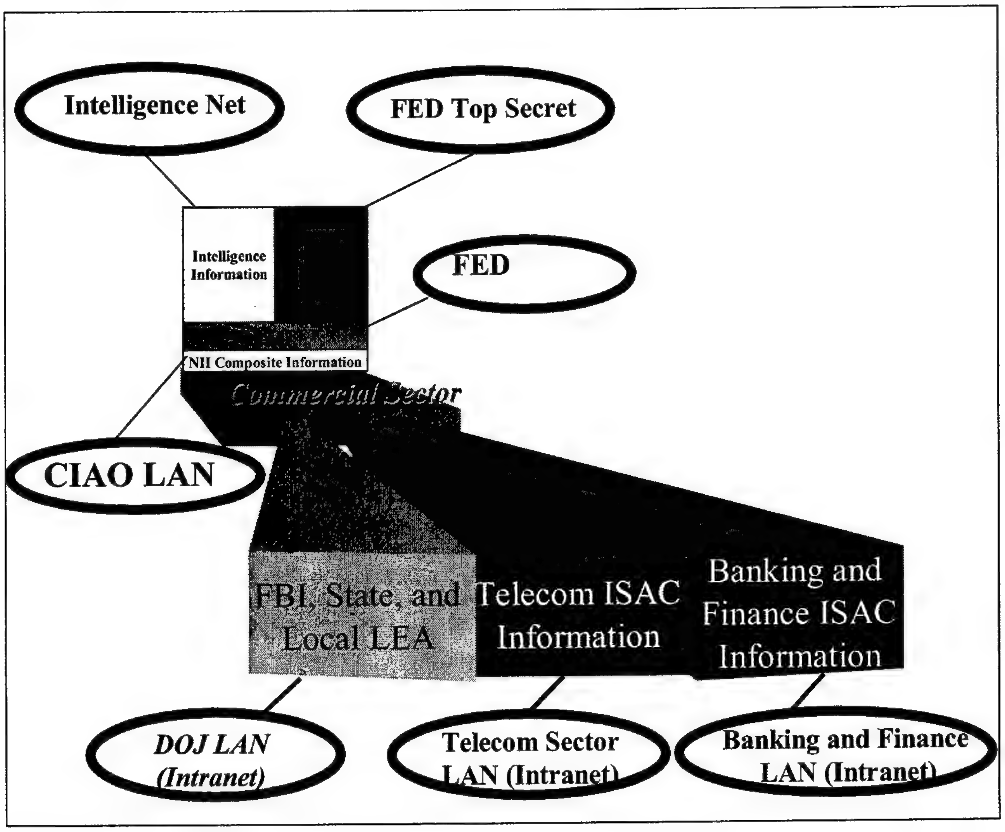

Intelligence Net
FED Top Secret
Intelligence Information
FED
NII Composite Information
Commercial Sector
CIAO LAN
FBI, State, and Local LEA
Telecom ISAC Information
Banking and Finance ISAC Information
DOJ LAN (Intranet)
Telecom Sector LAN (Intranet)
Banking and Finance LAN (Intranet)

Figure 7 - Example PDD Intranets: Detailed View

d) ***Multiple Level Security.*** Multiple Level Security (MLS) network refer to a network on which information and users of various level of confidentiality can be supported simultaneously with a reasonable level of trust that unintended exposures of information will not occur. The step to Multi-Level Security entails the ability to secure the LAN communications, allowing workstations of varying classification level to function on the same LAN.

Appendix B: The Sample Scenario Synopses

Before delving into the sample scenarios, it is important to re-iterate that these abbreviated scenarios are intended only to illustrate the concepts presented in the paper. They are not proposed as exhaustive or conclusive studies pertaining to the information sharing and security approaches in either case. However, within the narrow focus and the constraints of remaining unclassified, the scenario does try to be complete and accurate. Senior leadership from key stakeholders of both scenarios have reviewed, contributed to and commented on the paper.

Sample Scenario 1 allows the examination of a 'clean sheet' environment. Since the work in this area is just getting underway, objectives and requirements will be the focus of the study. The PDD example examines some of the underlying issues when sharing information between organizations. How does the picture change when your network's security approach must account for another independent organization's approach to security? The issue here is complicated by the fact that the uses of the information and the missions of the organizations are not common, nor are the organizational approaches to security the same.

In the Sample Scenario 2, GCCS has an established environment, culture, objectives, and de facto approach to sharing and security. The GCCS case study issues stem from the growing need for more information to be shared more efficiently within the organization at varying level of confidentiality. Conceptually, DOD accomplishes this by classifying the data as SECRET, TOP SECRET, and UNCLASSIFED, then providing labeling, handling, protection, sharing, and access processes and procedures. The GCCS ADP realization of this concept is separate networks at the various classification levels. However, the same issues would arise in any enterprise that has data to be shared with only a subset of the company (i.e., personnel data, customer data, pay data, etc), but for which there are some individuals (CEOs, network administrators, etc) that need access to more than one pool of data. These issues are complicated by the growing diversity, both mission and geographical, in organizational elements in today's networked environment.

Sample Scenario 1: Presidential Decision Directive (PDD) 62 and 63 at a Glance. With the challenges of information warfare, cyber terrorism, and cyber crime, the boundaries of the roles and responsibilities for protecting the national information infrastructure blur among law enforcement, intelligence, State, Defense, state governments, local governments, and the private sector. What is clear is that information needs will continue to broaden within a narrowing time frame and with increasingly overlapping and duplicating efforts. Growth comes at a moment when critical information resources are at a premium, pushed to the point where the burdens of collecting, analyzing, and disseminating information must be shared. How can sharing these burdens be addressed and the critical national information infrastructure protected?

Sample Scenario 1 Synopsis

With the challenges of information warfare, cyber terrorism, and cybercrime, the boundaries of the roles and responsibilities for protecting the national information infrastructure blur among law enforcement, intelligence, State, Defense, state governments, local governments, and the private sector. What is clear is that information needs will continue to broaden within a narrowing time frame and with increasingly overlapping and duplicating efforts. Growth comes at a moment when critical information resources are at a premium, pushed to the point where the burdens of collecting, analyzing, and disseminating information must be shared. How can sharing these burdens be addressed and the critical national information infrastructure protected?

> "*As we approach the 21st Century, our foes have extended the fields of battle from physical space to cyberspace; from the world's vast bodies of water to the complex workings of our own human bodies. Rather than invading our beaches and launching bombers, these adversaries may attempt cyberattacks against our critical military systems and our economic base.*
>
> – President William J Clinton, May 22, 1998[68]"

> "*Computers are changing our lives faster than any other invention in our history. Our society is becoming increasingly dependent on information technologies, which are changing at an amazing rate. ... We must ask whether we are becoming so dependent on communications links and electronic microprocessors that a determined adversary or terrorist could possibly shut down federal operations or damage the economy simply be attacking our computers.*
>
> – Senator Fred Thompson, May 19, 1988[69]"

The Question:

Is there a feasible approach to connect the major players and share key information electronically which will enable: detection, warning, and thwarting of attack; investigation and determination of response; and response and recovery?

Background

Executive Order 13010 established the President's Commission on Critical Infrastructure Protection (PCCIP) which was to examine eight sectors for security

[68] Zalmay Khalilzad and John White, "Strategic Appraisal: The Changing Role of Information in Warfare", Introduction, RAND, Project Air Force, @1999, RAND, Chapter one, page 7

[69] Zalmay Khalilzad and John White, "Strategic Appraisal: The Changing Role of Information in Warfare", Introduction, RAND, Project Air Force, @1999, RAND, Chapter one, page 7

vulnerabilities: telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services, and continuity of government. In response to the PCCIP, President Clinton signed PDD-62, Combatting Terrorism, and PDD –63, Critical Infrastructure Protection. The directives were designed to defend the nation's critical infrastructure from various threats, including "cyber attacks" by computer hackers and terrorists. The initial plan for implementation of PDD-63 was published January 2000. Concurrently and closely related, the effort to address the growing terrorism threat to the US. In response to this threat, President Clinton signed PDD 62.

Both these efforts call for new levels of cooperation and partnerships between the Federal Government, State Governments, Local Governments, local responders, and the private sector in accomplishing their respective tasks. The focus of this paper is on the information sharing and security approach for the inter-agency, inter-departmental, and inter-organizational interactions needed to support the anti-terrorism and infrastructure protection efforts, not on the actual terrorism or infrastructure protection questions themselves. This author makes the assumption that there will need to be some intranet-type, similar to the intelligence communities INTELINK, established in order to accommodate the information sharing required for the success of either of these PDD efforts. For example, this scenario is not looking at what organization A's individual IS&S approach should be (e.g., how they are protecting their own information, who they share information with in the course of doing business, etc). This scenario is looking at IS&S approach for the infrastructure supporting the reporting of attacks, the sharing of attack warnings, the sharing of information on threats and vulnerabilities, and the sharing of information on responses and possible fixes.

Sample Scenario 2: The Joint Command and Control Infrastructure. As information requirements and the volume of data grow, as concerns in information sharing and security broaden, as response times become shorter and shorter, and as "cyberthreats" and "information targets" expand, will the Department of Defense (DOD) need to balance information security and information sharing for its concepts for the 21st century to be feasible? Some areas come in for enormous discussion: Information Warfare, interoperability, Battlespace Dominance, Rapid Response, integration of air and space assets, combined Information Operations. But the element missing from these discussions is a clear and comprehensive, workable approach to information sharing and security: will the DOD's Joint Command and Control Infrastructure security approach meet the needs of tomorrow?

Sample Scenario 2 Synopses

In general, sample scenario two looks at the issues confidentiality levels in exiting organizations. As information requirements and the volume of data grow, as concerns in information sharing and security broaden, as response times become shorter and shorter, and as "cyberthreats" and "information targets" expand, will the Department of Defense (DOD) need to balance information security and information sharing for its concepts for the 21st century to be feasible? Some areas critical to our future war fighting capabilities are: Information Warfare, interoperability, Battlespace Dominance, Rapid Response, integration of air and space assets, combined Information Operations. But the element missing from these discussions is a clear and comprehensive, workable approach to information sharing and security: will the DOD's Joint Command and Control Infrastructure security approach meet the needs of tomorrow? Investigations have been unable to find a document, other than a few writings on data encryption and other specific solutions, that addresses how the security environment of today must evolve or change to meet DoD's information sharing demands of 2010, not even in the command and control arena.

The Question. The Joint Staff looks toward new business practices that require more and faster access to information; will its present approach to security still work? To illustrate the framework, we will limit the scope of the question to "Does the current ADP approach of separate LANs for separate levels of confidentially meet DoD's need for a common command and control system?" More specifically, examining the current Global Command and Control System/Global Combat Support System (GCCS/GCSS) security approach of maintaining separate security classification levels on disjoint, separate networks versus connecting or bridging the networks and employing a data confidentiality labeling scheme. For the purposes of this paper, discussion will be limited to objectives, stakeholders, stakes, trends, and assessments of whether the current bundling for electronic classified data will support future war fighting command and control business objectives. In addition, the unclassified nature of this paper also precludes detailed discussions.

Background

> *"Second, the information 'dimension' increasingly becomes central to the outcome of battles and campaigns. Therefore, protecting the effective and continuous operation of one's own information system and being able to degrade, destroy, or disrupt the functioning of the opponent's information system will become a major focus of the operational art.*[70] *"*

For clarity, Global Command and Control (GCC) is used in referring to the people, processes, procedures, tools, methods, and information involved in command and control. Global Command and Control System (GCCS) refers to the ADP-based information infrastructure and information system supporting GCC.

In both Joint Vision 2010 and in the Global Command and Control (GCC) concept of operations, GCCS is designated as the single command and control system from joint operations. It is comprised of over 700 sites with in excess of 10000 workstations and holds information on current operations, situational awareness, weather, intelligence, logistics, operation's planning, unit correspondence, DoD messages, and systems administration. However, at the joint level alone, there are four separate networks used on a daily basis for command and control – GCCS-SECRET, GCCS-TOP SECRET, a NORAD version of GCCS allowing for Canadian access, and the internet (UNCLASSIFIED), used heavily for logistics, communications with reserve and guard forces, and contacting agencies outside of DoD including contractors and support organizations. This approach requires someone with TOP SECRET Clearance to access three different networks, via three different workstations, logins, passwords, to see all the planning, logistics, or operational data pertaining to their job. Some units only have access to a single network, and no single network connects all the units.

DoD lacks a formal overall information sharing and security approach. Given that, and the interest of brevity, examination of the perceived difference between the hardcopy and electronic information labeling bundling will illustrate the needed concepts. At the architectural level, statutes and DoD regulations provided the needed high level framework for information classification labeling. As presented in NSA's accreditation guidance documents, DISA's SHADE documents and other DoD documentation, at the implementation level both bundling maintain the desire for at least paragraph level data classification labeling. However, in the electronic realizations, there is no explicit data labeling, and data security level is implied as the security classification level of the ADP system the information resides upon. However, for accessibility and availability reasons, most classified networks contain information from multiple security classification levels, up to and including the highest security level of the system. This has occurred due to the unavailability of adequate, economically feasible approaches to electronic data labeling. Similarly, the private sector faces similar issues, most prominently with e-commerce and e-business, but also in their basic business environments.

[70] Andrew W Marshall, "Strategic Appraisal: The Changing Role of Information in Warfare", <u>Forward</u>, RAND, Project Air Force, @1999, RAND, page 4-5

The existing GCC/GCS management structure provides an acceptable forum for information sharing and security approach development and implementation. The GCC/GCS Advisory Board is comprised on senior level stakeholder representatives and is chaired by the war fighting communities, the major stakeholder for command and control. However, that charter of the GCC Advisory Board, GCC Review Board, and GCC requirements Board must be modified to move information security requirements from technical requirements, prioritized and funded separately from business's functional requirements, to the functional requirements category.